UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Paulo Sérgio Ribeiro

Um Protocolo Criptográfico Para Comunicação Anônima Segura em Grupo

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.

Florianópolis, Fevereiro de 2003

Um Protocolo Criptográfico Para Comunicação Anônima Segura em Grupo

Paulo Sérgio Ribeiro

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Fernando Ostuni Gauthier, Dr.

Banca Examinadora

_____

Prof. Ricardo Felipe Custódio, Dr.

_____

Prof. Clóvis Torres Fernandes, Dr.

_____

Prof. Carlos Roberto De Rolt, Dr.

Ofereço esta Dissertação aos meus pais, Francisco e Dalva.

A concretização deste trabalho é um presente a eles.

Agradecimentos

Primeiro a Deus, por estar presente na minha trajetória.

Aos meus pais Francisco e Dalva, pelo empenho e dedicação, a quem devo todos os méritos da minha vida acadêmica.

A minha namorada Greice, pela compreensão e apoio.

Ao Departamento de Pós-graduação em Ciência da Computação da Universidade Federal de Santa Catarina (UFSC) e da Universidade do Estado de Santa Catarina (UDESC) pela qualidade do curso ministrado.

Ao LabSEC, Laboratório de Segurança em Computação da UFSC.

Ao meu orientador Prof. Dr. Ricardo Felipe Custódio, cujo conhecimento e a capacidade de motivar seus alunos extrapolam o conceito de mestre.

Aos colegas de mestrado, pela evolução conjunta alcançada, fruto do nosso convívio.

Agradeço a todos que direta ou indiretamente contribuíram para sucesso deste trabalho de pesquisa.

Sumário

Lista de Figuras **ix**

Notação **xi**

Resumo **xiii**

Abstract **xiv**

1 Introdução **1**

1.1 Contexto da Pesquisa 2

1.2 Objetivos 3

1.2.1 Objetivo Geral 3

1.2.2 Objetivos Específicos 5

1.3 Motivação 6

1.4 Trabalhos Correlacionados 8

1.5 Conteúdo Desta Dissertação 10

2 Fundamentos de Criptografia **11**

2.1 Introdução à Criptografia 12

2.2 Criptografia Simétrica 13

2.3 Criptografia Assimétrica 16

2.4 Chaves de Sessão 18

2.5 Função Resumo 19

2.6 Assinatura Digital 22

2.7 Assinatura às Cegas 25
2.8 Rede de Misturadores 27
2.9 Prova de Conhecimento-Zero 27
2.10 Compartilhamento de Segredo 29
2.11 Protocolos Criptográficos 30
2.12 Ferramentas Formais de Modelagem de Protocolos 32
2.12.1 Conceituação das Redes de Petri 34
2.12.2 Notação Gráfica das Redes de Petri 35
2.13 Conclusão 36

3 Comunicação de Grupo: Esquemas de Assinaturas em Grupo 37
3.1 Assinaturas em Grupo 38
3.2 Um Novo Esquema de Assinaturas em Grupo 41
3.3 Assinaturas em Grupo com Base na Identidade 42
3.4 Um Novo Esquema de Assinaturas em Grupo com Base na Identidade . . 44
3.4.1 O Esquema de Assinaturas em Grupo Proposto por Tseng e Jan . 45
3.4.2 Análise de Segurança do Esquema de Tseng e Jan 47
3.4.3 Comparação do Esquema de Tseng e Jan com o de Park, Kim e Won 48
3.5 Conclusão 49

4 Esquemas de Identificação 50
4.1 Introdução a Esquemas de Identificação 51
4.1.1 Comparativo entre Esquemas de Identificação e de Assinatura Digital 53
4.2 Esquemas de Assinatura Baseados na Identidade 55
4.3 Prova de Identidade Usando a Prova de Conhecimento-Zero 58
4.4 Esquemas de Identificação com Base no Logaritmo Discreto 60
4.5 Identificação Pelo Limiar 61
4.6 Transmissão Segura por Difusão 62

4.7 Conclusão 65

5 Protocolo Proposto 66

5.1 Contextualização do Assunto: Comunicação Anônima Segura em Grupo . 67

5.2 A Solução Apresentada 68

5.3 Protocolo Criptográfico: Comunicação Anônima Segura em Grupo 68

5.3.1 Considerações Sobre a Segurança do Protocolo Proposto 74

5.4 Funcionamento do Protocolo Proposto 76

5.5 Extensão do Protocolo Para Comunicação Anônima Segura em Grupo . . 78

5.5.1 Notação Específica Para Comunicação em Grupo 79

5.5.2 Distribuição das Chaves Para Comunicação Anônima Segura em Grupo 79

5.5.3 Considerações Sobre o Uso do Protocolo Para Comunicação Anônima Segura em Grupo 82

5.6 Conclusão 84

6 Análise de Segurança 85

6.1 Tipos de Ataques em Uma Rede de Comunicação de Dados 85

6.2 Segurança do Protocolo Proposto 88

6.2.1 Ataques à Disponibilidade 88

6.2.2 Ataques à Confidencialidade 88

6.2.3 Ataques à Integridade 90

6.2.4 Ataques à Autenticidade 90

6.2.5 Ataques ao Anonimato do Emissor 90

6.2.6 Considerações Sobre o Não-Repúdio do Emissor 90

6.3 Conclusão 91

7 Considerações Finais 92

7.1 Conclusões 92

7.2 Trabalhos Futuros 93

Referências Bibliográficas **95**

A Modelagem do Protocolo Proposto em Redes de Petri **98**

A.1 Descrição dos Elementos das Redes de Petri 99

A.2 Resultado Obtido 103

A.3 Conclusão 104

Lista de Figuras

2.1 Esquema de Criptografia Simétrica e Assimétrica 14
2.2 Processo de Cifrar e Decifrar Usando Chave Simétrica: Quando o Receptor Não Conhece a Chave K 14
2.3 Processo de Cifrar e Decifrar Usando Chave Simétrica: Quando o Receptor Conhece a Chave K 15
2.4 Processo de Cifrar e Decifrar Usando Chave Assimétrica 17
2.5 Aplicação da Chave de Sessão 19
2.6 Esquema de trabalho da Chave de Sessão 19
2.7 Processo de Cálculo do Resumo MD5 21
2.8 Processo de Cálculo e Transmissão do Resumo 22
2.9 Verificação da Integridade Pelo Resumo 22
2.10 Processo de Divulgação da Chave KU_A Pela Autoridade Confiável 24
2.11 Processo de Geração da Assinatura Digital 24
2.12 Processo de Verificação da Assinatura Digital 25
2.13 Exemplificação de Uso das Redes de Misturadores 28
2.14 Exemplo de Notação Gráfica da Rede de Petri 36

3.1 Primeiro Processo de Assinaturas em Grupo Proposto por Chaum e Heyst 39
3.2 Processo de Verificação das Assinaturas em Grupo 40

4.1 Ilustração dos Esquemas de Autenticação, Identificação e Assinatura . . . 55
4.2 Estrutura do Sistema Criptográfico Baseado na Identidade 57
4.3 Estrutura do Esquema de Assinatura Baseado na Identidade 58

4.4 Esquema de Difusão Por Transmissão Direta 63
4.5 Esquema de Difusão Por Subgrupo 64

5.1 Protocolo Criptográfico Para Comunicação Anônima Segura em Grupo . 69
5.2 Uso da Rede de Misturadores no Protocolo Proposto 74
5.3 Passo 5 com Chave Simétrica 78
5.4 Distribuição das Chaves no Grupo 80

6.1 Caracterização do Fluxo normal da informação 86
6.2 Caracterização do Ataque de Interrupção 86
6.3 Caracterização do Ataque de Interceptação 86
6.4 Caracterização do Ataque de Modificação 87
6.5 Caracterização do Ataque de Fabricação 87

A.1 Visualização Gráfica da Rede de Petri do Protocolo Proposto 99
A.2 Descrição dos Lugares e Transições em Linguagem ARP 105
A.3 Estrutura da Rede de Petri do Protocolo Proposto em ARP 106
A.4 Ilustração do Resultado da Compilação 107
A.5 Tela Apresentando o Estado Inicial da Rede 107
A.6 Transições Possíveis a Partir do Estado Inicial 108
A.7 Tela Apresentando a Chegada da Mensagem ao seu Destino 108

Notação

Alice (A)	Emissor da Mensagem
Beto (B)	Receptor da mensagem
Carol (C)	Terceira pessoa
Melo (M)	Uma pessoa maliciosa
Tiago (T)	Autoridade confiável
Simão (S)	Elemento responsável por embaralhar as mensagens
$\rightarrow$	Sentido de encaminhamento da Mensagem
$\triangleright$	Produz
$\Rightarrow$	Implica que
$\|\|$	Concatenação
X	Texto original, plano ou claro
Y	Texto cifrado
E	Cifrar
D	Decifrar
K	Chave usada para cifrar ou decifrar
$A \rightarrow B$	A envia mensagem ou chave para B
$E_K(X) \triangleright Y$	X cifrado com a chave K produz Y
$D_K(Y) \triangleright X$	Y decifrado com a chave K produz X
KU_i	Chave pública de i
KR_i	Chave privada de i
KS	Chave de sessão

$E_{KU_i}(X) \triangleright Y$	X cifrado com a chave KU_i produz Y
$D_{KR_i}(Y) \triangleright X$	Y decifrado com a chave KR_i produz X
$E_{KR_i}(X) \triangleright Y$	X cifrado com a chave KR_i produz Y
$D_{KU_i}(Y) \triangleright X$	Y decifrado com a chave KU_i produz X
K_1 e K_2	Par de chaves criptográficas simétricas ou assimétricas
K_{ij1} e K_{ij2}	Par de chaves K_1 e K_2, geradas por i para comunicação com j
$E_{K_1}(X) \triangleright Y$	X cifrado com a chave K_1 produz Y
$D_{K_2}(Y) \triangleright X$	Y decifrado com a chave K_2 produz X
N_i	Endereço físico de i
M	Mensagem não cifrada
ID_i	Identidade de i
$H(M)$	Resumo da mensagem M
H_{MD5}	Resumo da mensagem M calculado pelo MD5

Resumo

Esta dissertação aborda a comunicação segura entre os usuários de um canal aberto de comunicação de dados para uma situação específica. O objetivo é viabilizar um processo de comunicação que permita a usuários com interesses antagônicos ou concorrentes entre si, se comunicarem com total segurança, de maneira que um elemento receptor não possa expor um elemento emissor, em recebendo uma mensagem de forma segura. Isso é feito sem que se tenha que abdicar das garantias oferecidas pela assinatura digital.

Apresenta-se, então, um protocolo criptográfico para comunicação segura em grupo, com uma característica especial, que garanta o anonimato do emissor da mensagem, exceto para o receptor, que é o único elemento que terá conhecimento da origem da mensagem. Mesmo estando certo da identidade do emissor e da integridade da mensagem recebida, o receptor não tem como revelar a identidade do emissor para um terceiro.

Palavras Chave: Segurança, Criptografia, Comunicação em Grupo, Garantia de Anonimato

Abstract

This dissertation treats the secure communication between some group members, who are users of an open data communication system, in an particular situation. The objective is to make possible a communication process that turn available users with antagonistic interest or who are competing each other, to communicate in a secure way, in such a way that the receiver could not expose the sender, at receiving a secure message. This should be done without abdicating the assurances offered by the digital signature.

Them, we present a cryptographic protocol for secure communication in group, with a special feature, that assures the sender anonymity, except for the receiver, who is unique element who is able to identify the sender identity. And, even being sure about it, he can not reveal the sender identity to a third part.

Key Words: *Security, Cryptography, Group Communication, Anonymity Assurance*

Capítulo 1

Introdução

A história da criptografia tem uma forte relação com a história das guerras entre povos e nações. A arte de enganar e garantir a confidencialidade das informações, tornando-as obscuras aos inimigos, foi objeto de intenso estudo dos governos e dos militares em tempos de guerra. Porém, a literatura sobre o assunto seguiu o caminho oposto, sendo escassas nos períodos de conflito. As publicações vieram a tomar maior intensidade somente após 1967, ano em que começou a aparecer uma série de contribuições científicas. Em 1972 as publicações ainda não eram abundantes, porém algumas contribuições relevantes já se faziam presentes, culminando em 1975, quando Diffie e Hellman propuseram um novo estilo de criptografia, fazendo uso de chaves assimétricas [DIF 76]. A partir desta data, a criptografia tomou novos rumos, iniciando uma fase onde o número de discussões, propostas e contribuições se tornaram abundantes, vindas de várias partes do mundo. Em 1996, Schneier publicou o livro ”Criptografia Aplicada”[SCH 96a], um dos livros mais cultuados sobre criptografia da atualidade.

Nos dias atuais, a criptografia tem se tornado um instrumento imprescindível, dada a crescente necessidade de *segurança da informação* nas organizações, acompanhando o uso cada vez mais freqüente de sistemas distribuídos e de canais abertos de comunicação. O uso de um canal aberto de comunicação é extremamente eficiente e prático, a exemplo da Internet, porém, algumas precauções devem ser tomadas para não expor as informações, pessoas e corporações envolvidas. Esse é um dos principais moti-

vos pelos quais as técnicas de criptografia estão em evidência, sendo objeto de estudo das principais universidades, empresas e governos de todo mundo.

No Brasil, a criptografia está em plena ascensão, tanto do ponto de vista acadêmico como do ponto de vista socioeconômico, principalmente após a medida provisória $N^o\ 2.200-2$, de agosto de 2001. Essa medida objetiva regular o sistema nacional de certificação digital, tornando viável que os documentos eletrônicos tenham validade jurídica, fazendo com que a criptografia se torne um instrumento para um uso mais abrangente dos recursos da informática.

São inúmeras as aplicações da criptografia no mundo moderno, das quais podemos citar: acessos seguros a bancos por intermédio da Internet, compras em tempo real via Internet, eleições seguras fazendo uso de urnas eletrônicas, troca de mensagens de maneira que se garanta a confidencialidade e a integridade da informação, e mais uma infinidade de outras aplicações mais específicas, cuja abrangência inviabiliza enumerá-las todas. As várias técnicas da criptografia foram objeto de estudo desta pesquisa, em especial as de maior relevância para a proposta deste trabalho.

A seguir, apresenta-se as seções que compõem este capítulo introdutório:

Na Seção 1.1, faz-se uma contextualização desse trabalho de pesquisa.

Na Seção 1.2, faz-se a descrição dos objetivos gerais e específicos.

Na Seção 1.3, apresenta-se as principais motivações para o desenvolvimento desta pesquisa.

Na Seção 1.4, faz-se uma correlação do tema da pesquisa com alguns trabalhos publicados.

Faz-se então, na Seção 1.5, a descrição do conteúdo dos capítulos que o compõem.

1.1 Contexto da Pesquisa

Em um cenário típico, onde usuários interagem entre si através de um sistema aberto de comunicação de dados, as técnicas criptográficas vêm para tornar viável uma *comunicação segura* entre os diversos elementos que compartilham algum tipo de

recurso ou de informação. Entende-se comunicação segura como sendo a troca de mensagens entre os diversos elementos, de maneira que se garanta, computacionalmente, a confidencialidade, a autenticidade, a integridade e a irretratabilidade das informações trocadas.

Em uma comunicação segura entre um grupo de usuários, uma necessidade se faz presente. Usuários com interesses antagônicos ou concorrentes entre si, também necessitam se comunicarem através de um canal aberto de comunicação de dados com segurança. Porém, uma garantia adicional se faz necessária, para que um elemento receptor não possa expor um elemento emissor, em recebendo uma mensagem segura. Isso deve ser feito sem que se tenha que abdicar das garantias oferecidas pela assinatura digital, objeto de estudo da Seção 2.6.

No intento de propor uma alternativa de comunicação para atender a necessidade acima descrita, apresenta-se um protocolo criptográfico para comunicação segura em grupo, com uma característica especial, que garanta o anonimato do emissor da mensagem, exceto para o receptor. O único elemento que terá conhecimento da origem da mensagem é o receptor, para quem a mensagem é destinada. Mesmo estando certo da identidade do emissor e da integridade da mensagem recebida, o receptor não tem como revelar a identidade do emissor a um terceiro.

1.2 Objetivos

Esta seção apresenta os principais objetivos da pesquisa realizada, e resume o motivo da elaboração desta dissertação de mestrado. Os objetivos são apresentados em duas subseções, 1.2.1 e 1.2.2, descrevendo os objetivos gerais e específicos, respectivamente.

1.2.1 Objetivo Geral

O principal objetivo desse trabalho de pesquisa é especificar e analisar um protocolo criptográfico, que permita a comunicação segura entre um grupo de

usuários, com interesses opostos ou concorrentes entre si. Esses usuários compartilham um canal aberto de comunicação de dados, e a comunicação deve acontecer em consonância com as características descritas abaixo.

Apresentação Formal do Problema

O problema a ser resolvido nesse trabalho de pesquisa é apresentado da seguinte maneira:

> **Alice emite uma mensagem para Beto. Porém, Alice quer a garantia que, se Beto publicar a mensagem recebida de Alice, ele não tenha como provar que esta mensagem veio de Alice, mesmo Beto estando certo disso.**

Requisitos Básicos da Proposta

1. Cada elemento tem seu subgrupo, de tamanho variável e ilimitado, sendo que nenhum dos elementos conhece o grupo como um todo.
2. Apenas membros do subgrupo podem assinar as mensagens.
3. Apenas um elemento saberá quem é o emissor da mensagem.
4. Em caso de disputa, a identidade do emissor não tem como ser comprovada.

Algumas variações no processo darão alternativas de uso do protocolo que aqui se propõe:

- As mensagens podem ser enviadas diretamente de Alice para Beto.
- As mensagens podem ser enviadas para um grupo de pessoas simultaneamente, porém somente uma delas saberá a origem específica da mesma.
- As mensagens podem ser enviadas com ou sem a garantia de confidencialidade, em cada uma das situações acima.

Beto pode encaminhar a mensagem recebida de Alice para um terceiro, e não tem nada que o impeça de fazê-lo. Porém, Beto não tem como comprovar a origem

específica da mensagem. Sendo assim, o anonimato de Alice em relação a terceiros estará garantido. Qualquer que seja a situação, a identidade de Alice não poderá ser comprovada.

1.2.2 Objetivos Específicos

Os seguintes objetivos específicos foram considerados no trabalho:

- Apresentar um estudo das diversas técnicas criptográficas relevantes para a proposta deste trabalho.
- Identificar na literatura os temas que mais se identificam com a proposta deste trabalho de pesquisa.
- Fazer um estudo aprofundado de trabalhos relacionados com os temas específicos, no intento de identificar características que venham contribuir na idealização da proposta.
- Apresentar uma contextualização do assunto, e uma discussão detalhada do problema a ser resolvido.
- Especificar e analisar um protocolo criptográfico que torne viável um processo de comunicação anônima segura em grupo.
- Identificar os pontos fortes e fracos da proposta, com algumas sugestões de melhorias e de trabalhos futuros.
- Apresentar uma análise de segurança, verificando o comportamento do protocolo proposto mediante os ataques possíveis.
- Analisar o protocolo proposto utilizando um modelo formal, no intento de identificar possíveis entraves no funcionamento.

1.3 Motivação

A motivação, para elaboração desse trabalho de pesquisa, nasceu do desafio de tornar viável uma comunicação segura, em uma situação específica, onde os usuários de um sistema aberto de comunicação de dados são elementos que não podem confiar uns nos outros, e que, mesmo assim, precisam se comunicar de forma segura.

O protocolo proposto nesse trabalho de pesquisa pode ser usado nas seguintes situações:

1. Aplicações onde a origem específica não pode ser comprovada.

2. Situações onde o emissor quer a garantia de estar preservando seu anonimato, e o receptor quer a segurança de saber a origem específica da mensagem. Qualquer tipo de informação trocada pode, posteriormente, ser usada contra o próprio emissor.

As situações acima descritas podem ser ilustradas com alguns exemplos práticos, respectivamente relacionados a cada uma das situações descritas anteriormente, conforme descrito a seguir:

1. Existem algumas aplicações onde a identidade do emissor de uma determinada informação deve ser preservada, e que o receptor deve certificar a origem específica da informação recebida. São exemplos deste tipo de aplicação:

    - *Pagamento eletrônico via Internet* - Em sistemas de pagamento via Internet, o receptor ou elemento verificador deverá identificar emissor ou elemento que efetua o pagamento. Porém, a identidade do comprador deverá ser preservada, a exemplo do que acontece em situação de compra e venda com dinheiro em papel.
    - *Sistema de votação digital* - Analogamente ao item anterior, um sistema de votação digital necessitará desta característica especial. A urna eletrônica, ou elemento receptor da informação de voto, deverá identificar a origem específica do voto, para que possa validá-lo. Porém, em nenhuma hipótese, o

sistema deverá permitir que o elemento receptor comprove a identidade de uma informação de voto recebida.

- *Sistema de leilão público via Internet* - Um terceiro exemplo consiste de um sistema de que torne viável um leilão público via Internet. O elemento responsável pelo recebimento das propostas deverá identificar a origem específica das mensagens, ou propostas. Porém, esse elemento receptor não deverá ter como provar a quem pertence uma proposta específica, pois fazendo isso, o elemento receptor poderá manipular o leilão.

2. Uma outra situação é simbolizada pelos seguintes cenários típicos, onde a troca de informações confidenciais entre oponentes são constantes, e que uma garantia adicional se faz necessária. São exemplos deste tipo de cenário:

   - *Cenário político brasileiro* - Neste tipo de ambiente, composto por vários oponentes políticos que necessitam constantemente se comunicarem, e que as opiniões pessoais, as informações confidenciais trocadas e as pessoas envolvidas não podem ser expostas, sob pena dos fatos serem levados a público, caracterizando uma ação ilícita ou até mesmo um escândalo público. Para esse caso, um sistema de comunicação anônima segura em grupo, tal como proposto por este trabalho de pesquisa, apresenta-se como uma alternativa de comunicação bastante interessante.
   - *Empresas concorrentes* - Um outro cenário, onde o protocolo, proposto neste trabalho, seria uma alternativa interessante de comunicação, é representado por um ambiente composto por empresas concorrentes. O exemplo das empresas de telecomunicações no Brasil é um caso típico. Constantemente, essas empresas necessitam trocar informações relativas a interconexões, aluguéis de canais de comunicação, apresentação se soluções integradas, entre outras necessidades. Porém, as informações sigilosas trocadas entre essas empresas poderão vir a ser usadas contra elas próprias, caso não se tenha um canal seguro de comunicação, tal como aqui proposto.

A principal motivação para o desenvolvimento deste é a busca de uma solução viável e imediata para o problema da comunicação anônima segura em grupo, objetivando o atendimento das situações específicas, conforme exemplificado anteriormente.

1.4 Trabalhos Correlacionados

Alguns trabalhos relacionados ao tema *Comunicação Anônima Segura em Grupo* são apresentados a seguir, bem como uma breve explicação do motivo pelo qual esses trabalhos podem vir a ajudar na solução do problema apresentado na Seção 1.2.1. A discussão detalhada desses trabalhos, bem como de uma série de outras publicações científicas, será apresentada ao longo dessa dissertação.

Assinaturas em Grupo

Em 1991, o conceito de assinaturas em grupo foi introduzido por Chaum e Heyst [CHA 91]. Apresentou-se, ainda, quatro propostas de implementação das assinaturas em grupo.

Em 1994, Chen e Pedersen apresentaram um novo esquema de assinaturas em grupo, que oculta a identidade do assinante incondicionalmente e, contrariamente às propostas iniciais de Chaum e Heyst, permite novos membros serem inseridos no grupo [CHE 94]. Esse esquema é mais eficiente contra possíveis quebras de anonimato.

Em 1998, Yuh e Jinn apresentaram melhorias às propostas acima citadas, mantendo-se o anonimato de quaisquer outras assinaturas anteriores ou de futuras assinaturas [TSE 98].

Algumas características das assinaturas em grupo se assemelham com a proposta deste trabalho de pesquisa, uma vez que o protocolo a ser proposto prevê a comunicação entre um grupo de usuários, tratando também a questão do anonimato dos membros do grupo.

Assinatura às Cegas

Em 1982, Chaum propôs o primeiro esquema de assinatura às cegas, cujo objetivo é o de unir a confiabilidade da assinatura digital com a segurança do anonimato [CHA 83]. Essa proposta viabiliza assinar um documento sem conhecer seu conteúdo, e teve absoluta importância no desenvolvimento de protocolos para eleição segura e dinheiro digital, entre outros.

Em 2000, Chun, Wei e Yi publicaram uma proposta agregando alguns benefícios à proposta de Chaum, adicionando um fator randômico para proteger contra ataques que tentam descobrir a identidade dos membros [FAN 00].

A característica capaz de unir a confiabilidade da assinatura digital com a segurança do anonimato representa o principal desafio deste trabalho de pesquisa.

Problemas Não Resolvidos

Os temas acima relacionadas não são suficientes para a solução do problema, apresentado na Seção 1.2.1.

As assinaturas em grupo têm a seguinte característica: a identidade dos membros participantes são preservadas. Porém, em caso de disputa futura, pode ser revelada. Para a proposta deste trabalho de pesquisa, é necessário que a identidade do originador seja preservada antes, durante e depois de enviar as mensagens, exceto para o receptor.

A assinatura às cegas também trata a questão do anonimato. Em recebendo uma mensagem, o receptor não identifica a origem específica, porém ele sabe que a mensagem foi validada por uma Autoridade Confiável. Para a proposta deste trabalho de pesquisa, o anonimato do emissor é uma necessidade. Porém, diferente das propostas baseadas na assinatura às cegas, o elemento receptor deve identificar a origem específica da mensagem.

1.5 Conteúdo Desta Dissertação

No Capítulo 2, apresenta-se um resumo das diversas técnicas e esquemas criptográficos a serem aplicados, direta ou indiretamente, no protocolo proposto.

No Capítulo 3, apresenta-se os conceitos de assinaturas em grupo, e uma análise das principais publicações sobre o assunto.

No Capítulo 4, apresenta-se os conceitos relativos ao tema: Esquemas de Identificação.

No Capítulo 5, descreve-se detalhadamente o protocolo proposto, passo a passo.

No Capítulo 6, faz-se uma análise de segurança do protocolo proposto.

Finalmente, no Capítulo 7, faz-se as considerações finais sobre o trabalho de pesquisa realizado.

Faz-se ainda, no Apêndice A, a modelagem do protocolo proposto em *Redes de Petri*, visando analisar o seu funcionamento.

Capítulo 2

Fundamentos de Criptografia

Apresenta-se, neste capítulo, uma revisão literária dos principais fundamentos da criptografia. O objetivo é descrever alguns conceitos da criptografia, com os quais pôde-se aprofundar no trabalho de pesquisa, em busca de uma proposta capaz de tornar viável uma comunicação anônima segura entre um grupo de usuários.

Essa revisão começa na Seção 2.1, onde se introduz o conceito de criptografia. Na Seção 2.2, descrevem-se os conceitos de criptografia simétrica. Na Seção 2.3, apresentam-se os conceitos de criptografia assimétrica. Na Seção 2.4, enfoca-se a necessidade do uso de chaves de sessão. A Seção 2.5 esclarece a necessidade do uso de funções resumo para garantir a integridade da informação. Na Seção 2.6, apresentam-se os conceitos de assinatura digital, a garantia de autenticação e do não-repúdio. Na Seção 2.7, vêem-se os conceitos de assinatura às cegas, de fundamental importância para protocolos que necessitam de anonimato. Na Seção 2.8, apresenta-se a aplicação das redes de misturadores, como maneira de aumentar a garantia do anonimato. Na Seção 2.9, discorre-se sobre o conceito da Prova de Conhecimento-Zero, bastante usado em esquemas de identificação, objeto de estudo do Capítulo 4. Na Seção 2.10, descreve-se uma implementação necessária em sistemas que requerem uma segurança adicional: o compartilhamento de segredo. Na Seção 2.11, apresenta-se as definições e procedimentos para elaboração de protocolos criptográficos. Finalmente, na Seção 2.12, apresenta-se os conceitos de modelagem para protocolos criptográficos, enfatizando-se a técnica de

modelagem em Redes de Petri.

2.1 Introdução à Criptografia

Sistemas abertos de comunicação de dados, ou seja, onde um canal de comunicação é compartilhado por vários usuários ao mesmo tempo, são bastante difundidos na atualidade. Porém, algumas precauções devem ser tomadas para não expor as informações e os usuários envolvidos. Sem as adequações necessárias, alguns usuários maliciosos podem vir a burlar o propósito inicial deste tipo de sistema, acessando informações não autorizadas, recebendo mensagens não destinadas a ele, emitindo mensagens como sendo outro elemento, ou interceptando informações para que não cheguem a seu destino. Este tipo de acesso indevido ao sistema é caracterizado como um ataque. Os tipos de ataques são mais bem apresentados no Capítulo 6.

Considera-se, então, uma *mensagem segura* como sendo uma mensagem capaz de resistir aos possíveis tipo de ataques, característicos de sistemas abertos de comunicação de dados.

Define-se, então, criptografia como sendo a arte e ciência de manter as mensagens seguras, principalmente com relação ao sigilo de seu conteúdo, dificultando seu entendimento em caso de serem acessadas por usuários não autorizados. Porém, a confidencialidade é somente uma das inúmeras funções da criptografia. As funções mais importantes são as seguintes:

Confidencialidade - Garante que a informação transmitida por um elemento somente poderá ser acessada por pessoas autorizadas, ou seja, garante o sigilo da informação.

Autenticação - Deverá ser possível certificar a origem de uma mensagem específica.

Integridade - Deverá ser possível para o receptor verificar se a mensagem recebida não sofreu modificações desde sua origem.

Não-Repúdio - Um emissor não poderá negar uma mensagem por ele enviada.

Tempestividade - Esta função caracteriza-se em provar que um documento específico existia em uma determinada data e hora, e que não sofreu nenhuma alteração desde então.

Cifrar e decifrar são as maneiras mais comuns de obter segurança. Os processos de cifrar e decifrar, também conhecidos por cifradores e decifradores, respectivamente, fazem uso de algoritmos criptográficos. Os algoritmos criptográficos, com base em substituições, funções e operadores matemáticos, transformam textos na sua forma original, também conhecidos como planos ou claros, em textos cifrados. A idéia fundamental é tornar computacionalmente impraticável, para alguém não autorizado, recompor o texto original em posse do texto cifrado.

Toda segurança dos algoritmos criptográficos é baseada em chaves criptográficas. A chave é um parâmetro usado no processo de cifrar, independente do texto original. Um texto plano ou original cifrado por uma chave criptográfica genérica K_1 produz um texto cifrado. Somente possuindo uma outra chave genérica K_2 é que o receptor da mensagem conseguirá decifrar o texto, recuperando o texto original.

O algoritmo criptográfico pode ser simétrico ou assimétrico, dependendo do tipo de chave empregada: simétrica ou assimétrica. A diferença entre chaves criptográficas simétricas e assimétricas é a seguinte. Para chaves simétricas, a chave usada para cifrar, K_1, é igual à chave usada para decifrar, K_2, ou K_2 pode ser recomposta a partir de K_1. Para chaves assimétricas, uma mensagem cifrada com a chave K_1 somente poderá ser decifrada pela chave K_2, e vice-versa. A Figura 2.1 ilustra o processo de cifrar e decifrar, usando chaves criptográficas. Técnicas de criptografia que utilizam chaves simétricas e assimétricas serão apresentadas neste capítulo. Na seqüencia, apresenta-se algumas técnicas de criptografia, relevantes para a pesquisa realizada.

2.2 Criptografia Simétrica

A criptografia simétrica, também chamada de criptografia convencional, faz uso de chaves simétricas para cifrar e decifrar mensagens. Entende-se como

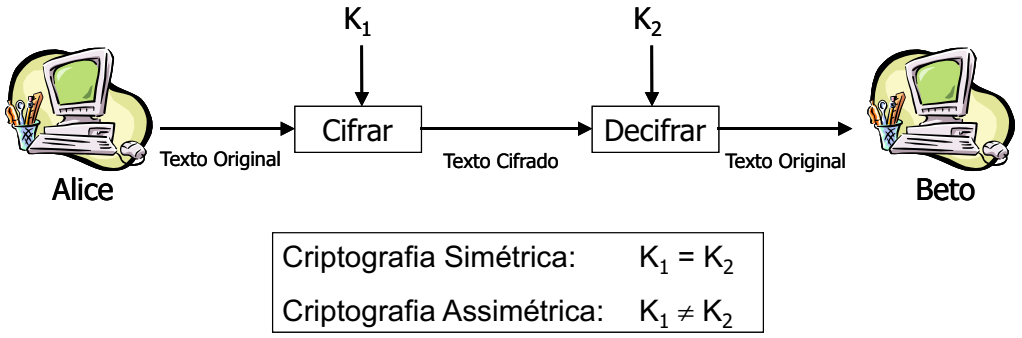

Figura 2.1: Esquema de Criptografia Simétrica e Assimétrica - Um texto plano ou original cifrado por uma chave criptográfica genérica K_1 produz um texto cifrado. O texto original é recomposto com a chave K_2.

chaves simétricas um par de chaves, de maneira que a chave usada para decifrar pode ser calculada a partir da chave usada para cifrar, e vice-versa. Na maioria dos algoritmos simétricos as chaves usadas para cifrar e decifrar são as mesmas. A Figura 2.2 ilustra um processo de criptografia usando chaves simétricas. Didaticamente, supõe-se que o cálculo

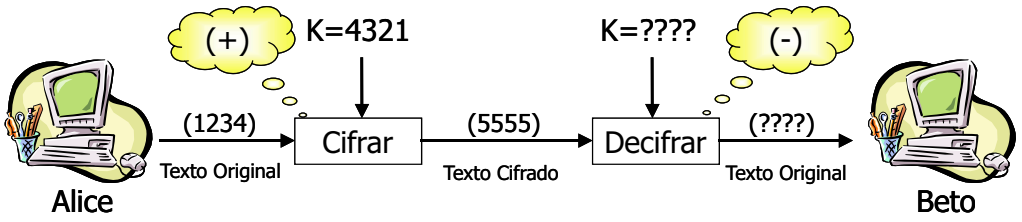

Figura 2.2: Processo de Cifrar e Decifrar Usando Chave Simétrica: Quando o Não Receptor Conhece a Chave K - Essa figura ilustra o processo de cifrar e decifrar, quando o receptor não conhece a chave K. Didaticamente, considera-se que o processo de cifrar é uma soma simples e o processo de decifrar é uma subtração.

usado para cifrar é uma soma simples e para decifrar é uma subtração. O texto e a chave são números de quatro algarismos. Sem o conhecimento da chave, o texto não pode ser decifrado, mesmo se conhecendo todos os outros fatores do sistema. No caso, tem-se o seguinte:

$$X = 1234$$

$$K = 4321$$
$$Y = E_K(X) = E_{4321}(1234) = 4321 + 1234 \Rightarrow Y = 5555$$

Sem conhecer a chave K, e mesmo sabendo que o processo de decifrar é uma subtração simples, o receptor da mensagem não consegue decifrá-la:

$$X = D_K(Y) = D_{????}5555 = 5555 - ???? \Rightarrow X = ????$$

A Figura 2.3 ilustra o mesmo processo, porém o destinatário, Beto, conhece a chave que será usada para decifrar. Quando o receptor conhece a chave K, basta

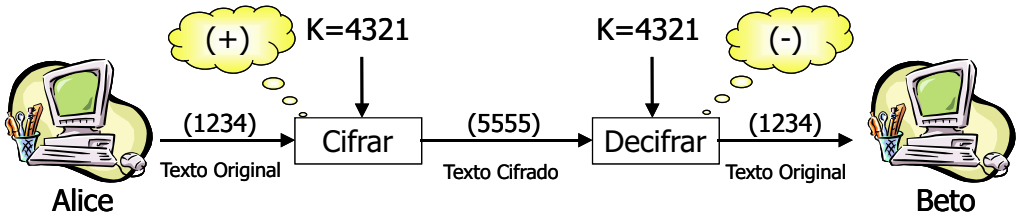

Figura 2.3: Processo de Cifrar e Decifrar Usando Chave Simétrica: Quando o Receptor Conhece a Chave K - Essa figura ilustra o processo de cifrar e decifrar, quando o receptor conhece a chave K. Didaticamente, considera-se que o processo de cifrar é uma soma simples e o processo de decifrar é uma subtração.

que ele execute a operação usada para decifrar, que no exemplo é uma subtração simples, para recuperar o texto original ou plano. Nesta segunda situação, o texto original é recuperado pelo receptor da mensagem, pois agora o receptor conhece a chave K:

$$X = D_K(Y) = D_{4321}5555 = 5555 - 4321 \Rightarrow X = 1234$$

Vale observar que o uso de uma soma para cifrar e de uma subtração para decifrar é apenas didático, sendo que a função matemática usada nesses processos são bem mais complexas e com características bastante específicas, cujo objetivo único é dificultar ao máximo as tentativas de recuperação do texto original por pessoas não autorizadas. A diferença entre as diversas funções matemáticas usadas para cifrar e decifrar

mensagens é o que define e caracteriza um algoritmo criptográfico.

Como exemplo de algoritmos de criptografia simétricos pode-se citar [STA 99]:

- Triple DES [DES 85]
- IDEA [LAI 90]
- Blowfish [SCH 94]
- RC5 [RIV 95]
- CAST [ADA 93]
- RC2 [RIV 97]

Dos fundamentos da criptografia simétrica constatou-se a seguinte característica [SCH 96a]:

> ”Criptografia simétrica provê alguma autenticação. Quando Beto recebe uma mensagem de Alice cifrada com a chave compartilhada entre eles, Beto sabe que a mensagem veio de Alice. Ninguém mais conhece a chave usada por eles. No entanto, Beto não tem como convencer um terceiro sobre isso.”

Esta característica, citada por Schneier como um problema da criptografia simétrica, representa uma importante funcionalidade a ser considerada no protocolo que aqui se propõe.

2.3 Criptografia Assimétrica

Em 1976, Diffie e Hellman mudaram os rumos da criptografia ao apresentar o que eles chamaram de criptografia de chave pública, também conhecida como criptografia assimétrica [DIF 76]. Diferente da criptografia tradicional, eles propuseram um esquema que usa duas chaves distintas, denominadas chaves assimétricas. Uma das chaves é publicada, chamada chave pública, e a outra é mantida em segredo, chamada

chave privada. Essas chaves são usadas para cifrar mensagens, de maneira que uma mensagem cifrada com a chave privada somente poderá ser decifrada com a chave pública, e vice-versa.

A Figura 2.4 ilustra o processo de cifrar e decifrar usando chaves assimétricas, visando garantir confidencialidade. Considerando que o texto original é 1234,

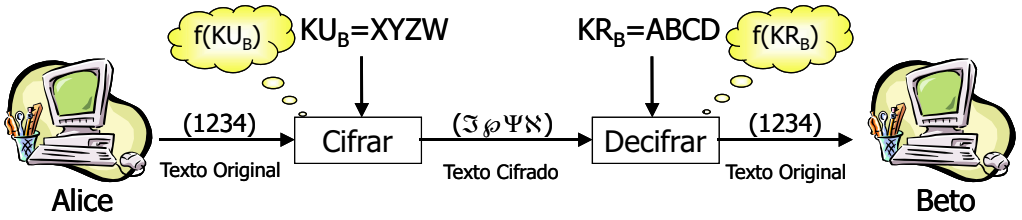

Figura 2.4: Processo de Cifrar e Decifrar Usando Chave Assimétrica - Essa figura ilustra o processo de criptografia assimétrica, visando a confidencialidade.

um processo de cifrar é feito em função da chave pública $KU_B = XYZW$, de maneira que o texto transmitido, cifrado, fica ininteligível e só pode ser decifrado pelo destino, que conhece a chave privada $KR_B = ABCD$. Na criptografia assimétrica, é computacionalmente muito difícil descobrir a chave privada a partir da chave pública.

Nos dias atuais, um dos algoritmos criptográficos mais usados é o RSA [RIV 78], que é uma implementação dos conceitos de chaves assimétricas. Os passos descritos a seguir sintetizam o algoritmo RSA:

1. Selecionar dois números primos p e q, como por exemplo $p = 7$ e $q = 17$.

2. Calcular $n = p \times q$. Exemplo: $n = 7 \times 17 => n = 119$.

3. Calcular $\Phi(n) = (p - 1) \times (q - 1)$. Exemplo: $\Phi(n) = 96$.

4. Selecionar e de maneira que e seja relativamente primo a $\Phi(n)$ e menor que $\Phi(n)$. Por exemplo: $e = 5$.

5. Determinar d de maneira que $d \times e = 1 \bmod \Phi(n)$, sendo d menor que $\Phi(n)$. Por exemplo: $d = 77$, porque $77 \times 5 = 385 = 4 \times 96 + 1 = 1 \bmod 96$.

6. Como resultado, obtém-se a chave pública $KU = \{e, n\}$ e a chave privada $KR = \{d, n\}$. No exemplo: $KU = \{5, 119\}$ e $KR = \{77, 119\}$.

O processo de cifrar usando-se a chave pública é feito para uma mensagem M, sendo M menor que n e o texto cifrado C é obtido calculando $C = M^e$ mod n. Para decifrar, basta calcular $M = C^d$ mod n. Supondo $M = 100$, tem-se o seguinte:

$$C = M^e \text{ mod } n = 100^5 \text{ mod } 119 = 53$$

Para recuperar a mensagem M, faz-se o seguinte:

$$M = C^d \text{ mod } n = 53^{77} \text{ mod } 119 = 100$$

Os fundamentos e as propriedades da matemática modular, que nos auxiliam em cálculos tais como acima demonstrado, podem ser encontrados em [SCH 96a] ou [STA 99].

Uma vez que a mensagem M está cifrada com a chave privada KR, recuperar M sem o conhecimento da chave pública KU é um problema de difícil solução computacional. Levaria-se muitos anos para que a recuperação pudesse se dar.

2.4 Chaves de Sessão

O algoritmo de chave pública não é um substituto para a criptografia simétrica [SCH 96a]. Os algoritmos de chave pública são lentos e necessitam de chaves grandes, para que não fiquem vulneráveis a alguns ataques. Na maioria das implementações práticas, a criptografia de chave pública é usada para a distribuição segura da chave simétrica, durante a sessão de interação entre emissor e receptor. Por isso, essa chave simétrica é chamada *chave de sessão*. Essa chave de sessão é que será efetivamente usada para cifrar as mensagens [KOH 78]. Esta técnica se baseia em o emissor gerar uma chave KS simétrica de sessão, cifrar essa chave usando a chave assimétrica

pública do receptor, e enviá-la para o receptor. O receptor decifra a mensagem recuperando a chave KS. A chave KS será usada para a comunicação efetiva entre ambos. A Figura 2.5 ilustra o uso das chaves assimétricas para distribuição das chaves simétricas, sendo que esta última é usada para cifrar e decifrar as mensagens.

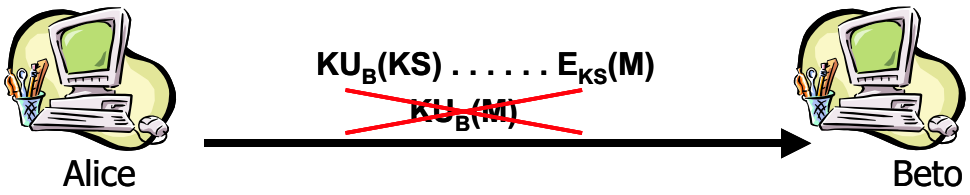

Figura 2.5: Aplicação da Chave de Sessão - Ao invés de cifrar a mensagem usando a chave pública KU_B, o que se faz é usar a chave KU_B para distribuição segura da chave simétrica de sessão KS. Dessa maneira, a chave KS será efetivamente usada para cifrar a mensagem.

A Figura 2.6 ilustra o processo de transmissão de uma mensagem fazendo uso da chave de sessão.

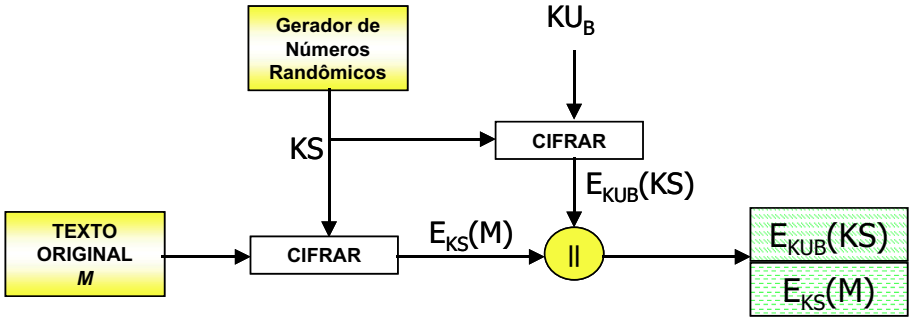

Figura 2.6: Esquema de trabalho da Chave de Sessão - Essa figura representa o processo de transmissão da chave KS, cifrada com KU_B, e da mensagem M cifra com KS.

2.5 Função Resumo

A função resumo ou função *Hash* é usada para garantir a integridade da informação. Esse processo consiste em obter um valor de tamanho fixo, calculado em

função de uma mensagem genérica, de tamanho qualquer. Este valor, chamado resumo ou *Hash* da mensagem, é anexado à mensagem original, agregando uma informação redundante, com o objetivo de atestar a integridade da mensagem. As propriedades da função resumo são as seguintes [STA 99]:

- A função resumo pode ser aplicada sobre uma mensagem de qualquer tamanho.
- A função resumo produz uma saída de tamanho fixo.
- O resumo de uma determinada mensagem é fácil de ser calculado.
- Para um dado resumo, é computacionalmente impraticável achar a mensagem que produziu esse valor. Por esta característica, a função resumo também é conhecida como função de caminho único.
- É bastante improvável que a função resumo aplicada a duas mensagens distintas gere um mesmo valor.
- É computacionalmente impraticável encontrar duas mensagens distintas que produzem um mesmo resumo.

A seguir apresenta-se exemplos de algoritmos usados para produzir o resumo, também conhecidos por algoritmos *Hash* [STA 99]:

1. **MD5 -** O MD5 (*Message-Digest Algorithm*) foi desenvolvido por Rivest no MIT (*Massachusetts Institute of Technology*). O MD5 se tornou um padrão em 1992, RFC 1321 (*Network Working Group - Request for Comments: 1321*).
2. **SHA -** O SHA foi desenvolvido pelo NIST (*National Institute of Standards and Technology*) e publicado na FIPS (*Federal Information Processing Standard*) em 1993. A versão revisada foi editada em 1995 e denominada SHA-1.
3. **RIPMED-160 -** O RIPMED-160 foi desenvolvido em função de uma pesquisa, que lançava ataques parcialmente bem sucedidos ao MD5, como parte do projeto RIPE (*RACE Integrity Primitives Evaluation*), em 1996.

4. **HMAC** - O HMAC (*Keyed-Hashing for Message Authentication*) tornou-se um padrão em 1997, RFC 2104 (*Network Working Group - Request for Comments: 2104*).

Na Figura 2.7, ilustra-se o processo de cálculo do resumo usado no MD5. Nesse algoritmo, a mensagem de tamanho genérico $Kbits$ é segmentada em n blocos de 512 bits, Y_0 à Y_{n-1}, sendo o último bloco, Y_{n-1}, é preenchido com $100000...000$ até completar os 512 bits. Cada bloco de 512 bits é submetido a uma função cuja entrada é o resultado do último bloco calculado. A primeira entrada é um número 128 bits aleatórios. Como resultado final, obtém-se um resumo da mensagem, $H(M)$, com um tamanho fixo de 128 bits.

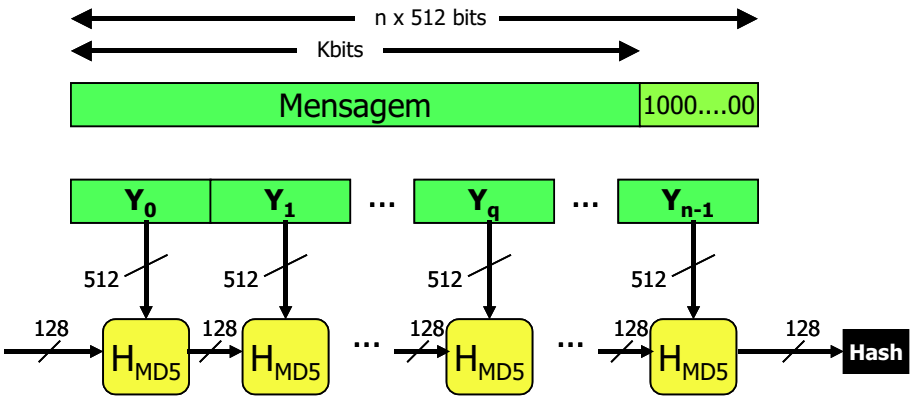

Figura 2.7: Processo de Cálculo do Resumo MD5 - Essa figura representa o processo de cálculo do resumo, utilizado no MD5, para uma mensagem de tamanho genérico $Kbits$. Como resultado, obtém-se o resumo da mensagem M, sempre de 128 bits.

A Figura 2.8 ilustra o processo de transmissão da mensagem e do resumo da mensagem, como sendo uma informação redundante da mensagem, permitindo verificar a integridade da mesma no destino.

A Figura 2.9 representa a maneira que a integridade da mensagem é verificada. O resumo é recalculado no destino e comparado com o resumo transmitido, verificando assim a integridade da informação transmitida. Qualquer alteração na mensagem ou no resumo transmitido é constatada com esta verificação.

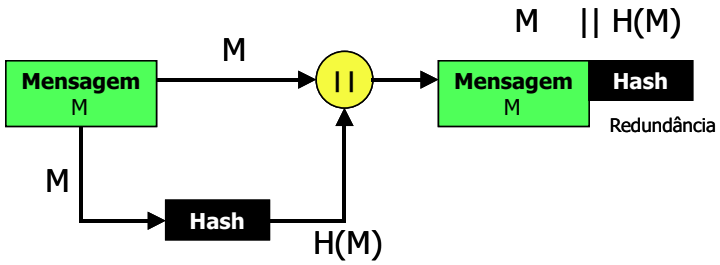

Figura 2.8: Processo de Cálculo e Transmissão do Resumo - Essa figura apresenta o processo de cálculo e transmissão do resumo, como uma redundância da mensagem. O resumo é transmitido com a mensagem M.

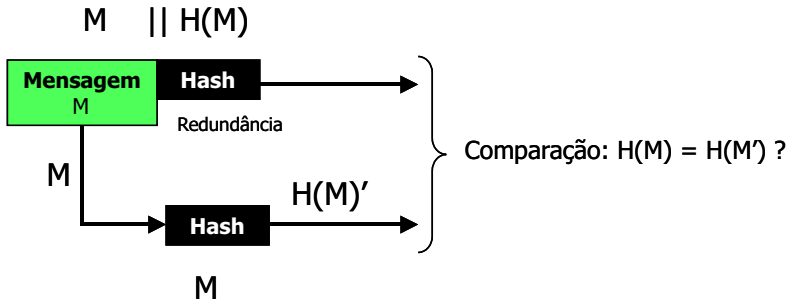

Figura 2.9: Verificação da Integridade Pelo Resumo - No processo de verificação, uma vez recebida a mensagem M e o resumo $H(M)$, o destinatário calcula novamente o resumo da mensagem, $H'(M)$, e compara com o resumo recebido, $H(M)$.

A função resumo é usada no processo de geração de uma assinatura digital, conforme apresentado a seguir.

2.6 Assinatura Digital

As características da assinatura digital são semelhantes à assinatura manual, que vem sendo usada como prova de autoria ao longo dos tempos, ou até mesmo como uma concordância a um determinado documento [SCH 96a]. As seguintes funções criptográficas são consideradas neste caso:

- *Autenticidade* - A assinatura digital convence o receptor que o documento foi realmente assinado pelo emissor. A assinatura é a prova de que o emissor é o signatário

do documento, e ninguém mais.

- *Não-reuso* - A assinatura não pode ser removida de um documento e passada para outro.

- *Integridade* - Após assinado, o documento não pode ser alterado.

- *Não-repúdio* - O signatário não pode, futuramente, reivindicar que não foi ele quem assinou o documento.

A assinatura digital é a aplicação das características acima relacionadas em um documento eletrônico. O uso de chaves assimétricas possibilitou o desenvolvimento de novos conceitos de assinatura digital. O NIST (*National Institute of Standards and Technology*) publicou um padrão para o uso da assinatura digital, conhecido como DSS (*Digital Signature Standard*), inicialmente proposto em 1991 [STA 99], que usa criptografia assimétrica e funções resumo, tal como descrito na Seção 2.5, agregando uma garantia de integridade ao esquema.

As características de autenticidade e não-repúdio são garantidas através do uso de uma Autoridade Confiável, responsável pela distribuição segura das chaves públicas, e da criptografia assimétrica. A Figura 2.10 ilustra o processo de divulgação da chave pública de Alice KU_A. Alice gera um par de chaves assimétricas KU_A e KR_A. A chave pública KU_A é encaminhada por um canal seguro até uma Autoridade Confiável, que tem a função de distribuir esta chave, atestando que ela pertence realmente a Alice. A chave privada KR_A é mantida em segredo por Alice, e será usada para cifrar a mensagem M enviada por Alice. A Autoridade Confiável é responsável por validar e atestar a chave pública de Alice.

A Figura 2.11 descreve um processo de assinatura de uma mensagem genérica. A assinatura consiste em cifrar o resumo da mensagem com a chave privada de Alice, KR_A. O resumo original pode ser recomposto com a chave pública de Alice, KU_A. Como a chave privada de Alice é de conhecimento exclusivo de Alice, o receptor, de posse da chave KU_A previamente divulgada pela Autoridade Confiável, tem certeza

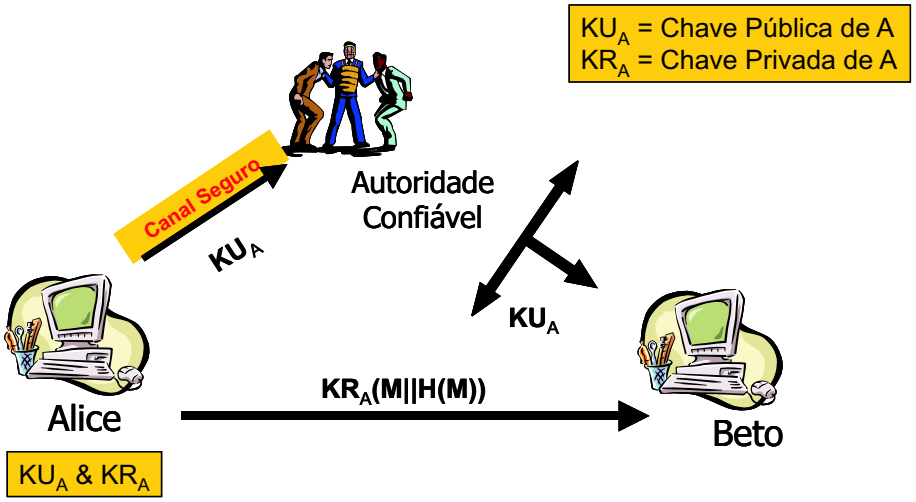

Figura 2.10: Processo de Divulgação da Chave KU_A Pela Autoridade Confiável - Essa figura representa o processo de divulgação da chave pública de Alice, KU_A por uma Autoridade Confiável.

de que a mensagem veio mesmo de Alice, e com a garantia de integridade dada pelo resumo. O resultado do processo de assinatura de Alice é válido somente para a mensagem específica. Esse processo é usado quando se deseja apenas assinar a mensagem, sem a garantia de confidencialidade.

Existe ainda uma maneira prática de garantir sigilo da mensagem assinada, essa alternativa consiste em Alice cifrar a mensagem assinada, $E_{KR_A}(H(M))\|M$ com a chave pública de Beto, KU_B, como demonstrado a seguir. Neste caso, somente

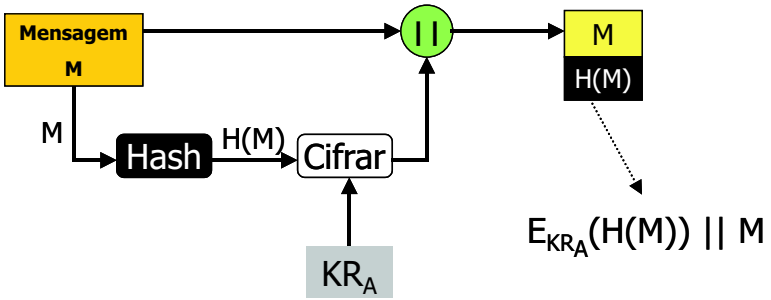

Figura 2.11: Processo de Geração da Assinatura Digital - Esse processo consiste em cifrar o resumo com KR_A e transmitir juntamente com a mensagem M.

Beto, que possui a chave KR_B terá acesso ao conteúdo da mensagem.

$$A \rightarrow B : E_{KU_B}(E_{KR_A}(H(M))\|M)$$

Na fase de verificação da assinatura digital, o resumo é decifrado no destino, usando a chave pública de Alice, KU_A. O processo de verificação do resumo é feito recalculando o resumo da mensagem recebida e comparando com o resumo recebido. Com isso, a integridade da mensagem é validada. O processo é ilustrado na Figura 2.12.

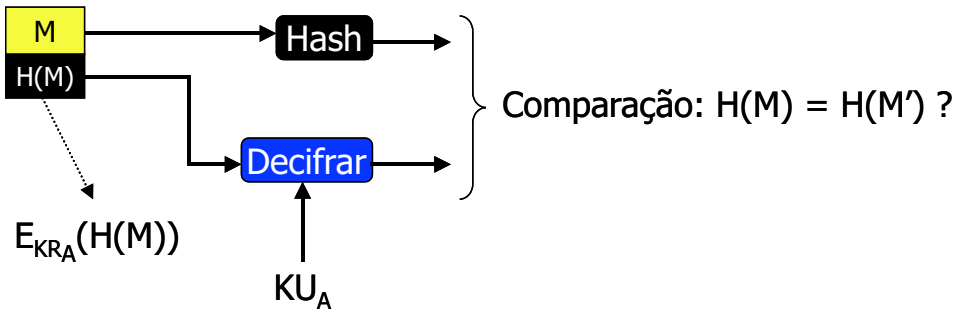

Figura 2.12: Processo de Verificação da Assinatura Digital - Nesse processo, o resumo $H(M)$ é decifrado no destino, usando KU_A. A verificação é feita comparando o resumo recebido, $H(M)$, com o resumo recalculado sobre a mensagem M recebida, $H(M')$.

A funcionalidade de não-reuso da assinatura é garantida pela característica de o resumo ser associado à mensagem. Desta maneira, essa assinatura é válida somente para a mensagem em questão.

2.7 Assinatura às Cegas

Uma das principais características da assinatura digital é que o signatário saiba o que ele está assinando. Esta é uma boa idéia, exceto quando se necessita do oposto.

Baseado no RSA, Chaum propôs o primeiro esquema de assinatura às cegas [CHA 83]. Suponha que Tiago é uma autoridade pública. Alice quer que Tiago assine um documento sem conhecer seu conteúdo. Tiago não se preocupa com o conteúdo,

pois ele está apenas certificando que foi notificado em um determinado horário. Após feito o processo de assinatura às cegas, Alice terá um documento assinado por Tiago, sem que ele saiba o conteúdo.

Tiago poderá verificar a validade da assinatura sempre que o documento assinado for mostrado a ele.

O processo utilizado para obtenção da assinatura às cegas pode ser representado pelos seguintes passos [SCH 96a]:

1. Tiago tem uma chave pública e, uma chave privada d e um módulo público n. Alice quer que Tiago assine a mensagem M sem conhecer seu conteúdo.

2. Alice gera um número aleatório k, entre 1 e n. Então Alice encoberta a mensagem M, calculando:

   $$t = Mk^e \text{ mod } n$$

3. Tiago assina t:

   $$t^d = (Mk^e)^d \text{ mod } n$$

4. Alice recupera t^d calculando o seguinte:

   $$s = t^d/k \text{ mod } n$$

5. O resultado desta operação é este:

   $$s = M^d \text{ mod } n$$

   A operação feita para obtenção deste resultado é a seguinte:

   $t^d = (Mk^e)^d = M^d k \text{ mod } n$, então

   $t^d/k = M^d k/k = M^d \text{ mod } n$

Desta maneira, consegue-se ter M assinado por Tiago, sem que ele conheça o conteúdo da mensagem.

Esta técnica tem suma importância no desenvolvimento de protocolos onde a necessidade do anonimato está presente, como no caso de eleição segura e dinheiro digital, entre outros.

2.8 Rede de Misturadores

A Rede de Misturadores é uma estrutura criptográfica, que objetiva aumentar a segurança de aplicações, onde o anonimato é uma necessidade [CHA 81]. Suponha que um elemento esteja monitorando os canais de comunicações de maneira maliciosa, em um sistema de comunicação genérico. Fazendo isto, esse elemento poderá associar o endereço do emissor ao do receptor, bem como ao tamanho das mensagens enviadas e recebidas, e descobrir que Alice está se comunicando com Beto, por exemplo.

A Rede de Misturadores tem como objetivo mascarar o endereço físico do emissor, bem como, eliminar qualquer relação estatística entre o tamanho das mensagens emitidas e recebidas.

A Rede de Misturadores é um elemento confiável, cuja função fundamental é a de encaminhar as mensagens recebidas em fragmentos. Desta maneira, ao invés de Alice encaminhar a mensagem diretamente para Beto, ela encaminha para esse elemento intermediário, a Rede de Misturadores, que passa a mensagem assim fragmentada a Beto.

A Figura 2.13 ilustra o uso da Rede de Misturadores, aumentando a segurança e a garantia do anonimato de Alice.

2.9 Prova de Conhecimento-Zero

Schneier ilustra o protocolo *Prova de Conhecimento-Zero*, necessário para o entendimento dos esquemas de identificação apresentados no Capítulo 4, com o seguinte diálogo didático [SCH 96a]:

Alice: - Eu sei a senha secreta do sistema de computação da Reserva Militar Federal.

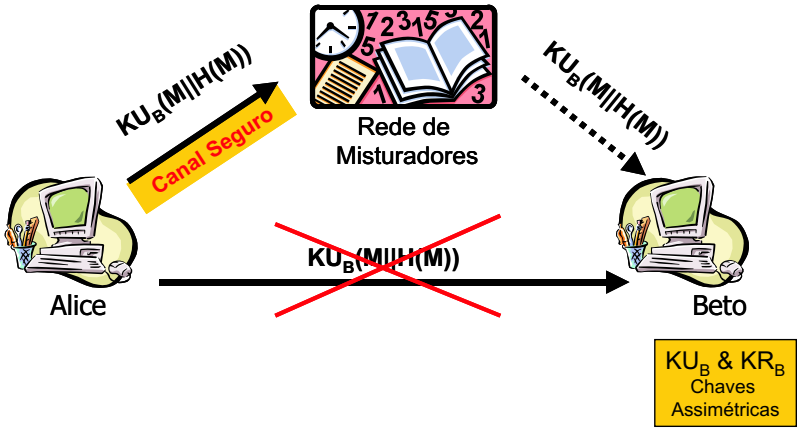

Figura 2.13: Exemplificação de Uso das Redes de Misturadores - Essa figura exemplifica o uso das Redes de Misturadores, um elemento intermediário que repassa as mensagens recebidas de Alice para Beto, de maneira fragmentada, conforme representado pelas linhas tracejadas.

Beto: - Você não sabe.

Alice: - Sim, eu sei.

Beto: - Então prove.

Alice: - A senha secreta é ...

Beto: - Legal, agora vou publicá-la no *The Washington Posts*.

Alice: - Epa!!!

A idéia da *Prova de Conhecimento-Zero* foi introduzida em 1985 por Goldwasser, Micali e Rackoff. e tem a seguinte característica [GOL 85]. Alice e Beto fazem uso de um protocolo interativo. Beto faz uma série de questões para Alice. Se Alice souber o segredo, ela responderá corretamente. Se Alice não souber, ela terá 50% de chance de responder corretamente, por exemplo. Após 10 perguntas, por exemplo, Beto estará convencido de que Alice sabe realmente o segredo, sendo que nenhuma das respostas dadas a Beto contém informações que o permitam descobrir o segredo.

O nome Prova de Conhecimento-Zero se deve ao fato do protocolo viabilizar que Beto saiba se Alice conhece um determinado segredo, sem que Alice tenha que divulgar o conteúdo desse segredo.

2.10 Compartilhamento de Segredo

Em um sistema de comunicação aberto, é importante restringir o acesso a algumas informações confidenciais. Isso pode ser feito com uma chave criptográfica, onde o conhecimento da chave permite o acesso à informação. No entanto, em uma situação com exigência de um grau mais elevado de segurança, o manuseio de uma chave única se torna crítico, e é em casos assim que o esquema desta seção aparece como solução. O termo *compartilhamento de segredo* se refere ao compartilhamento das informações sigilosas necessárias para o acesso à informação, ou seja, ao compartilhamento das chaves criptográficas.

Um grau de segurança maior pode ser obtido dividindo a chave criptográfica por um grupo de participantes. O conceito de compartilhamento de segredo foi introduzido por Shamir [SHA 79] e Blakley [BLA 79] em 1979. O esquema proposto por eles é um método onde n partes do segredo é distribuída entre os n participantes. Um sub grupo de t partes pode reconstituir o segredo, de tal forma que o seguinte ocorra:

- O segredo pode ser recomposto com o conhecimento de t partes, sendo t um subgrupo de n.
- O segredo não pode ser recomposto com o conhecimento de menos que t partes.

Nessa proposta, faz-se necessário o auxílio de uma Autoridade Confiável, que é o elemento com a função de distribuir as n partes do segredo para os elementos. Existem situações mais específicas, onde não se pode confiar nem mesmo em uma Autoridade Confiável que conheça todas as chaves secretas. Ingemarsson e Simmons apresentaram uma proposta de esquema de compartilhamento de segredo sem o uso de uma Autoridade Confiável para o cálculo das chaves a serem formadas [ING 90].

Os conceitos acima descritos, para o contexto deste trabalho, ficam apenas em caráter ilustrativo. Esta técnica não se aplica para a proposta desta pesquisa, uma vez que o termo *compartilhamento de segredo* se refere a compartilhar partes de uma chave criptográfica entre vários elementos de um grupo. Para evitar confusão, a proposta deste trabalho de pesquisa fica melhor descrita como a necessidade de compartilhar mensagens confidenciais, e não segredos, entre usuários, de forma segura.

2.11 Protocolos Criptográficos

Schneier define protocolo como sendo uma série de passos, envolvendo duas ou mais partes, destinados a cumprir uma tarefa [SCH 96a]. Em outras palavras, um protocolo se destina a estabelecer regras que permitam, duas ou mais partes, interagirem para a solução de um problema. São características de um protocolo genérico o seguinte:

- O protocolo tem uma seqüência definida, com início e fim.
- São necessárias duas ou mais partes para se ter um protocolo.
- Todos os envolvidos no protocolo devem conhecê-lo, bem como todos os passos a serem seguidos.
- Todos envolvidos no protocolo devem concordar em segui-lo.
- Cada passo do protocolo deve ser bem definido, não dando margens a duplo sentido de interpretação.
- Um protocolo deve ser completo, ou seja, todas as alternativas, situações e interações possíveis devem ser previstas.

Especificamente para sistemas de comunicação de dados, protocolo pode ser definido como sendo um conjunto de regras e convenções que definem meios para possibilitar a comunicação entre dois ou mais elementos. Esses elementos podem ser usuários finais, processadores ou sistemas de computação. Em protocolos criptográficos, pelo menos parte de uma mensagem é cifrada. Protocolos criptográficos, em resumo, são usados

para estabelecer uma comunicação segura através de um canal de comunicação aberto e em sistemas distribuídos.

Um protocolo criptográfico, que represente uma solução completa para um determinado problema, pode fazer uso de uma ou mais técnicas criptográficas. Fazendo uso das técnicas estudadas neste capítulo, pode-se estabelecer o seguinte procedimento para definição ou projeto de protocolos criptográficos:

1. Definição do problema específico a ser resolvido.
2. Definição de uma notação padrão para a formalização do protocolo específico.
3. Dar nomes aos diversos elementos que participarão direta ou indiretamente do protocolo.
4. O protocolo criptográfico específico é organizado em passos, sendo que cada passo representa uma das duas situações: processamento de informações feito por uma ou mais partes, ou mensagens trocadas entre as partes.
5. Fazer a análise de segurança, para avaliar a efetividade do protocolo.
6. Fazer uma modelagem formal do protocolo, para melhor avaliação do funcionamento do mesmo.
7. Por fim, fazer a avaliação e as considerações finais da proposta, demonstrando os pontos fortes e fracos.

Esse procedimento é o que foi usado no projeto do protocolo criptográfico, alvo deste trabalho de pesquisa.

Na modelagem formal do protocolo proposto, fez-se uso de Redes de Petri.

Por fim, uma definição de protocolo se faz necessária neste trabalho de pesquisa. É a definição de *protocolos interativos*. Protocolos interativos caracterizam pela constante troca de informações, do tipo pergunta e resposta, também chamadas interações, entre os elementos participantes. Em outras palavras, nos protocolos interativos, uma

série de interações se fazem necessárias para que se cumpra uma tarefa única, como por exemplo, a identificação do usuário de um sistema aberto de comunicação de dados, ou a verificação de uma determinada assinatura digital pelo elemento receptor.

2.12 Ferramentas Formais de Modelagem de Protocolos

Alguns métodos formais, com respectivas ferramentas de suporte, podem auxiliar na elaboração, análise e validação de um protocolo criptográfico, objetivando garantir a comunicação segura em sistemas abertos e em sistemas distribuídos. Esses tipos de sistemas são vulneráveis a intrusos, que tentam de alguma maneira subverter os propósitos do protocolo criptográfico.

Com isto, não é surpresa que vários protocolos criptográficos já publicados foram, posteriormente, vistos com uma série de falhas. Após a descoberta de uma falha, normalmente, ela é corrigida. No intento de antecipar as falhas encontradas, alguns pesquisadores desenvolveram métodos formais para a descoberta antecipada dos problemas, seguindo uma análise de aproximação, na busca do desenvolvimento de protocolos criptográficos cada vez mais efetivos.

Uma divisão dos tipos de técnicas de modelagem pode ser feita, válidas tanto para protocolos criptográficos como para protocolos de comunicação convencionais [GRI 99]:

- *Método de construção de inferência* - Este tipo de método é amplamente usado, e é baseado na construção de inferências utilizando lógicas especializadas.

- *Método de construção de ataque* - Este tipo de método é baseado na tentativa de simulação de possíveis ataques, aproveitando as propriedades algébricas dos algoritmos usados nos protocolos.

Os métodos formais têm como base modelos estruturais, os quais podem ser classificados como a seguir [LEE 97]:

- *Modelos Algébricos* - Este tipo de modelo baseia-se em regras algébricas [DOL 83], [LON 92], [WOO 91].

- *Modelos Lógicos* - O modelo BAN (Burrows-Abadi-Needham) baseia-se na lógica de autenticação e constitui um exemplo de modelo lógico [BUR 90]. Porém. esse tipo de modelo possui algumas limitações no que diz respeito à dificuldade nas especificações do protocolo e, também, por não considerar as propriedades temporais e semânticas do protocolo.

- *Modelos Lógicos e Algébricos* - Uma especificação unificando os modelos lógicos e algébricos foi proposta em [SNE 92].

- *Modelos Algébricos e Estado de Transição* - O comparativo destes tipos de modelos é sintetizado em [KEM 94]. No entanto, esse tipo de modelo possui alguns problemas, tais como a limitação na especificação de importantes características dos protocolos, a saber, paralelismo, não-determinismo e não-sincronismo, e impossibilidade de especificar propriedades matemáticas, entre outras.

- *Modelos em Redes de Petri* - Introduzido em 1962, com Redes de Petri obteve-se sucesso na modelagem e análise de sistemas onde a concorrência, o paralelismo e o não-sincronismo eram características presentes [PET 81]. Desde então, este modelo vem sendo difundido, tornando-se objeto de estudo de vários pesquisadores ao longo dos anos. Em 1990, começou a ser aplicado em sistemas seguros de comunicação de dados [VAR 90].

O formalismo das Redes de Petri possibilita a análise precisa do modelo, verificando as propriedades inerentes aos sistemas concorrentes, tais como relações de precedência entre eventos, sincronização e existência de bloqueio. Além de todas estas vantagens, permite a visualização dos processos e a comunicação entre eles.

Em função das características acima descritas, suficientes para análise do protocolo quanto à ocorrência de possíveis bloqueios na ocorrência seqüencial dos eventos, faz-se, neste trabalho de pesquisa, o uso das Redes de Petri para modelagem do protocolo proposto, no Apêndice A.

Faz-se, então, nas subseções seguintes, um estudo mais aprofundado das Redes de Petri. Na Subseção 2.12.1, apresenta-se os principais conceitos das Redes

de Petri. Faz-se ainda, na Subseção 2.12.2, a apresentação da gráfica das Redes de Petri.

2.12.1 Conceituação das Redes de Petri

As Redes de Petri constituem um modelo do tipo estado-evento, onde cada evento possui pré-condições que vão permitir sua ocorrência, e pós-condições decorrentes destas, as quais são, por sua vez, pré-condições de outros eventos posteriores. Outra característica importante, as Redes de Petri permitem a análise da estrutura e do comportamento dinâmico do sistema modelado.

As Redes de Petri são formadas por dois tipos de componentes: um ativo, denominado de *transição*, e outro passivo, denominado *lugar*. Os *lugares* correspondem às variáveis de estado, e as *transições*, às ações ou eventos, realizados pelo sistema.

A interligação entre os dois tipos de componentes é feita através dos arcos, definindo as condições que por sua vez possibilitam a execução das ações. As definições dos componentes da Rede de Petri são as seguintes:

Estado - Condição em que se encontra o sistema, em um instante específico.

Evento - Ocorrências que acarretam mudança de estado.

Condições - Atributos associados aos eventos e que definem a sua ocorrência.

Lugares (P) - Cada nó lugar corresponde ao depósito dos atributos, ou condições para a ocorrência de um ou mais eventos, representado por círculos.

Notação formal: $P = \{p_1, p_2, p_3, ..., p_n\}$

Transições (T) - O nó transição modela a ocorrência de um evento, representado por barras ou retângulos.

Notação formal: $T = \{t_1, t_2, t_3, ..., t_m\}$

Arco Orientado (Arc) - Que interliga um lugar a uma transição ou vice-versa, encadeando condições para a ocorrência dos eventos. O conjunto dos arcos está contido na união dos conjuntos $(P \times T)$ e $(T \times P)$.

Notação formal: $Arc \subseteq (P \times T) \cup (T \times P)$.

Marca ou Ficha - Representa um recurso disponível para ocorrência de um evento. O posicionamento dessas fichas, em alguns lugares da rede, constitui a marcação. A evolução da marcação permite modelar o comportamento dinâmico do sistema.

Marcação Inicial - Representa a condição inicial das fichas no sistema.

Notação formal: $M_0 = \{x_1, x_2, x_3, ..., x_n\}$

Sendo que x_1 corresponde ao estado inicial de p_1, x_2 corresponde ao estado inicial de p_2, etc.

2.12.2 Notação Gráfica das Redes de Petri

Faz-se, a seguir, um comparativo da notação formal com a notação gráfica, tomando-se como exemplo a seguinte notação formal:

$$P = \{p_1, p_2, p_3, p_4\}$$
$$T = \{t_1, t_2\}$$
$$Arc = \{(p_1, t_1), (p_2, t_2), (p_3, t_2), (t_1, p_4), (t_2, p_4)\}$$
$$M_0 = \{1, 1, 1, 0\}$$

A representação gráfica do modelo acima descrito está representada na Figura 2.14. Os círculos maiores representam os lugares, os retângulos, as transições, as setas, os arcos orientados, e os círculos pretos menores, as fichas.

Tomando a Figura 2.14 como referência, pode-se observar uma importante característica das Redes de Petri: a ocorrência da transição t_1 está condicionada à existência de fichas em p_1 e p_2; somente assim a transição se efetivará, transferindo a ficha para p_4.

Algumas extensões do modelo original foram desenvolvidas, como por exemplo: Redes de Petri envolvendo tempo, Redes de Petri Coloridas e Redes de Petri Criptográficas [CAR 97].

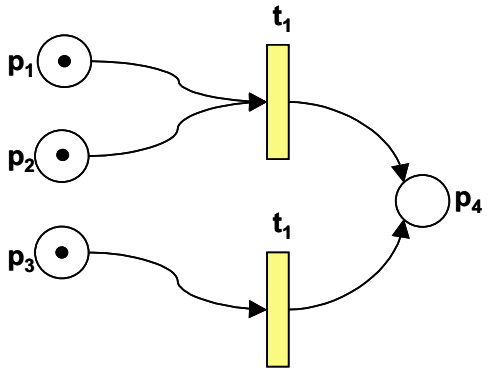

Figura 2.14: Exemplo de Notação Gráfica da Rede de Petri - Essa figura apresenta a notação gráfica da Rede de Petri a ser usada para modelagem do protocolo proposto.

A modelagem do protocolo proposto em Redes de Petri será apresentada no Apêndice A.

2.13 Conclusão

Apresentou-se, neste capítulo, os fundamentos da criptografia. A busca de uma solução para o problema da comunicação anônima segura em grupo, passa pelo estudo detalhado de cada uma das técnicas descritas neste capítulo.

Discutiu-se também os fundamentos para elaboração de protocolos criptográficos e, com base nos conceitos estudados, será elaborado um protocolo criptográfico que torne viável uma comunicação anônima segura em grupo.

Fez-se, ainda, a apresentação de algumas ferramentas de modelagem, utilizadas para avaliação de protocolos criptográficos, enfatizando as Redes de Petri, com as quais o protocolo proposto neste trabalho de pesquisa será modelado.

Esse capítulo, além se servir como uma sólida base sobre os fundamentos da criptografia, servirá como sustentação para compreensão dos capítulos seguintes.

Capítulo 3

Comunicação de Grupo: Esquemas de Assinaturas em Grupo

Este capítulo objetiva discutir os aspectos da comunicação em grupo, em especial de *Assinaturas em Grupo*, assunto de relevância para o problema e a proposta de solução oferecida por este trabalho de pesquisa.

A discussão do assunto em questão se faz com a apresentação e análise das principais técnicas de Assinaturas em Grupo da literatura. O objetivo é identificar algumas características que venham a auxiliar na elaboração de um protocolo criptográfico, para que se torne viável uma comunicação anônima segura entre um grupo de usuários concorrentes entre si, conforme problema apresentado na Seção 1.2.

Na Seção 3.1, o conceito de Assinaturas em Grupo é introduzido por Chaum e Heyst. Na Seção 3.2, apresenta-se novas propostas de esquemas de Assinaturas em Grupo. Na Seção 3.3, um esquema de Assinaturas em Grupo com base na identidade é apresentado. Por fim, na Seção 3.4, um novo esquema de Assinaturas em Grupo com base na identidade é discutido, bem como um comparativo com as propostas anteriormente apresentadas neste capítulo. As considerações finais são feitas na Seção 3.5.

3.1 Assinaturas em Grupo

Em 1991 Chaum e Heyst apresentaram um novo tipo de assinatura destinada à comunicação entre um grupo de pessoas, denominada Assinaturas em Grupo [CHA 91]. Esse esquema permite que membros ou elementos de um grupo possam assinar mensagens em favor do grupo. As seguintes propriedades são apresentadas:

- Apenas membros do grupo podem assinar mensagens.
- O receptor da mensagem pode verificar que esta é uma assinatura válida para o grupo, porém não pode descobrir a qual dos membros do grupo ela pertence.
- Em caso de disputa futura, ou seja, se por algum motivo houver necessidade futura de identificar o membro que emitiu uma determinada mensagem, a assinatura pode ser aberta, com ou sem a ajuda dos membros individuais do grupo, revelando a identidade do emissor.

Em resumo, cada membro do grupo convence os outros elementos que ele pertence ao grupo, sem revelar sua identidade.

Além de introduzir o conceito de assinaturas em grupo, Chaum e Heyst apresentaram quatro alternativas de implementação que satisfazem as propriedades acima.

Na primeira proposta de Chaum e Heyst, uma Autoridade Confiável, T, escolhe uma lista de chaves secretas para cada elemento ou membro do grupo, publicando-as em uma lista global [CHA 91]. As chaves secretas escolhidas por T não têm relação nenhuma com os membros do grupo. As chaves da lista são distribuídas para os elementos que participarão do processo de assinaturas em grupo. Esse processo está ilustrado na Figura 3.1.

Cada elemento pode assinar mensagens com uma chave secreta da lista, e o receptor poderá comparar essa assinatura com uma das chaves correspondentes na lista. Cada chave poderá ser usada apenas uma única vez. A Autoridade Confiável, T, conhece a lista de chaves públicas, podendo identificar quem produziu a assinatura. Na Figura 3.2, o processo de verificação da assinatura está ilustrado. Supondo que o Elemento

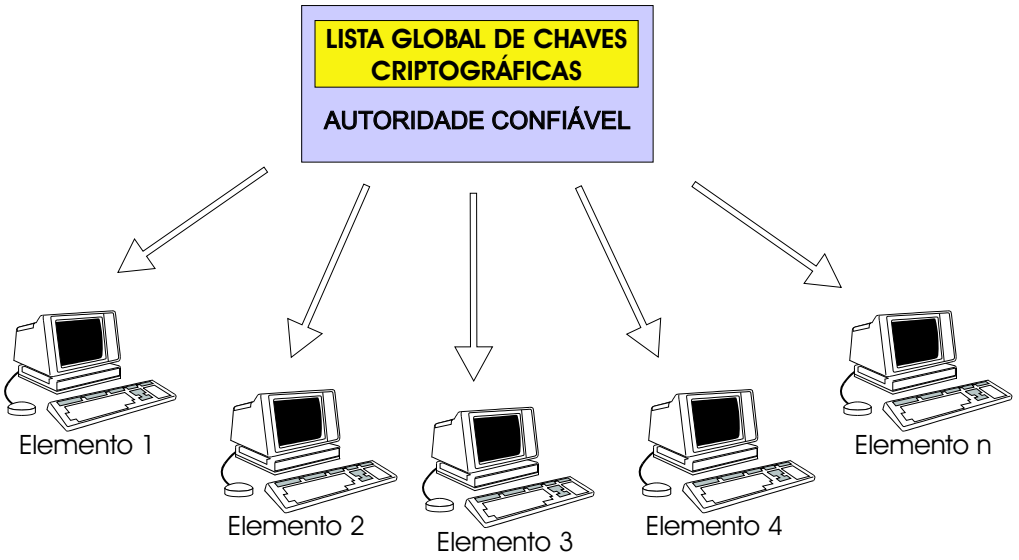

Figura 3.1: Primeiro Processo de Assinaturas em Grupo Proposto por Chaum e Heyst - Essa figura representa o primeiro processo de Assinaturas em Grupo proposto por Chaum e Heyst em 1991. Uma lista global de chaves criptográficas é mantida pela autoridade confiável. As chaves são distribuídas para os elemento que participarão do processo de assinaturas em grupo.

2 receba uma mensagem do Elemento 1, o mesmo poderá verificar, junto à Autoridade Confiável, T, na Lista Global de Chaves Criptográficas, certificando se a mensagem é oriunda de um dos membros do grupo. Somente T poderá identificar o emissor, caso seja necessário.

O problema com esse protocolo é que T conhece todas as chaves, podendo criar qualquer assinatura. Isso pode ser resolvido utilizando-se um processo de *Assinatura às Cegas*, conforme estudado na Seção 2.7. Com este avanço, T não poderá mais falsificar assinaturas, e cada membro possuirá apenas uma chave secreta.

Outra alternativa de implementação da primeira proposta de Chaum e Heyst é sugerida. Cada elemento do grupo envia chaves públicas para a lista global, mantendo a chave privada em segredo, e, com a garantia de que somente membros do grupo podem enviá-las, as funcionalidades do protocolo são preservadas.

Uma segunda proposta é apresentada por Chaum e Heyst. Nessa segunda alternativa de implementação, a Autoridade Confiável T distribui uma chave se-

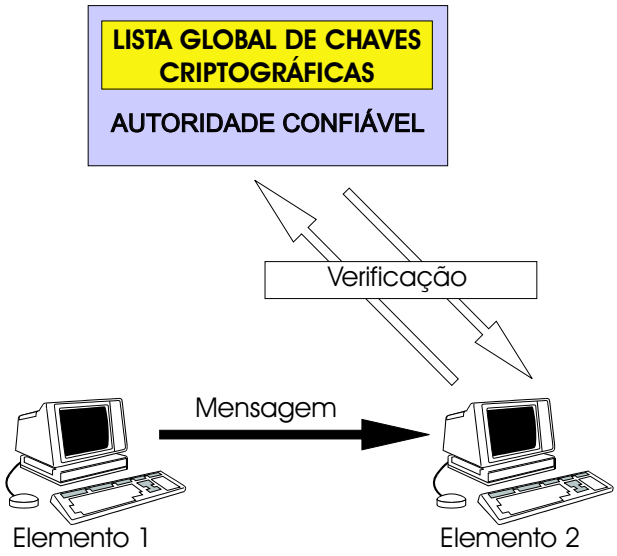

Figura 3.2: Processo de Verificação das Assinaturas em Grupo - Essa é a representação do processo de verificação das Assinaturas em Grupo da primeira proposta de Chaum e Heyst em 1991. Em recebendo uma mensagem vinda do elemento 1, o elemento 2 verifica junto à Autoridade Confiável a validade da assinatura.

creta para cada um dos membros, juntamente com uma chave pública, de conhecimento comum a todos os membros. As chaves secretas distribuídas por T possuem algumas condições especiais, de maneira que, utilizando-se algumas propriedades matemáticas, a validade das assinaturas feitas com essas chaves podem ser comprovadas, fazendo uso da chave pública previamente divulgada por T.

Supondo-se que Alice e Beto sejam elementos do grupo, e que, Alice emite uma mensagem para Beto. Beto, por sua vez, deve verificar a assinatura de Alice. Para que Beto identifique uma assinatura como sendo válida para o grupo, um protocolo interativo de confirmação deve ser executado, ou seja, faz-se necessária uma série de interações entre Alice e Beto, até que Beto esteja convencido de que a mensagem é de um membro do grupo, sem que a identidade de Alice seja revelada. Esse processo de verificação é feito sem a intervenção de T.

Como desvantagem desta proposta, se todos os membros, exceto um, conspirarem, a chave desse último pode ser revelada. Esse problema pode ser eliminado fazendo T como sendo um dos membros do grupo.

Chaum e Heyst apresentaram mais duas propostas, que satisfazem as necessidades para obtenção das Assinaturas em Grupo [CHA 91].

As propostas apresentadas por Chaum e Heyst vêm sendo objeto de constante estudo pelos pesquisadores da área, e melhorias têm sido apresentadas ao longo dos tempos. A seguir, apresenta-se algumas alternativas de implementação, fundamentadas no conceito por eles introduzido.

3.2 Um Novo Esquema de Assinaturas em Grupo

Chen e Pedersen [CHE 94] apresentam um novo esquema de Assinaturas em Grupo, que representa uma sensível melhoria às propostas de Chaum e Heyst [CHA 91]. A implementação sugerida por Chem e Pedersen oculta a identidade do assinante incondicionalmente e permite que novos membros possam ser inseridos no grupo. Em adição, esse esquema é mais eficiente contra possíveis tentativas de quebra de anonimato. Outro avanço é que, a Autoridade Confiável identifica o signatário usando um método que simplifica três dos esquemas apresentados por Chaum e Heyst.

Chen e Pedersen fazem a identificação de algumas características importantes a serem observadas nas assinaturas em grupo. São as seguintes:

- Identificação do signatário pela Autoridade Confiável: a Autoridade Confiável, T, deve ser capaz de identificar o assinante baseando-se na assinatura, na chave pública ou alguma informação secreta auxiliar.

- Adição e exclusão de membros: deve ser possível modificar o grupo dinamicamente, ou seja, um novo membro no grupo deve apenas requerer uma chave e uma identificação para a Autoridade Confiável. Nenhum dos quatro esquemas propostos por Chaum e Heyst respeitam esta propriedade.

Na proposta de implementação das assinaturas em grupo de Chen e Pedersen o grupo pode ser alterado dinamicamente. A Autoridade Confiável pode identificar cada membro, com alguma informação adicional. Para identificar o membro, usa-se um

processo de dupla assinatura, que permite identificá-lo mais facilmente, sem a necessidade de repetidas interações no processo verificação das assinaturas em grupo.

3.3 Assinaturas em Grupo com Base na Identidade

Uma outra maneira de implementar as assinaturas em grupo foi apresentada por Park, Kim e Won [PAR 97]. Eles propuseram um esquema de assinaturas em grupo que se baseia na identidade do emissor, de maneira que as assinaturas em grupo são verificadas a partir desta identidade dos membros. Identidade são informações particulares que identificam e diferenciam um membro do grupo dos demais. Na Seção 4.2 o conceito de identidade é tratado com maior profundidade. Sendo assim, as assinaturas em grupo, com base na identidade, consistem em um emissor, membro do grupo, ser identificado pela Autoridade Confiável pela sua identidade. Esse emissor comprova ser um membro do grupo provando conhecer a assinatura correspondente a este grupo.

Para a proposta de Park, Kim e Won, considera-se os seguintes quatro tipos de participantes:

- *Centro Confiável* - Responsável pela geração da assinatura dos diversos membros.
- *Autoridade do Grupo* - Responsável por identificar o signatário como sendo membro do grupo.
- *Signatário* - Membro do grupo que gera a assinatura pelo grupo.
- *Receptor* - Quem recebe a assinatura e verifica a validade da mesma.

No esquema proposto, o signatário tem apenas uma chave secreta para ambas assinaturas, ordinária ou pessoal e pelo grupo.

Compõe-se o esquema proposto por Park, Kim e Won nas seis etapas seguintes:

1. *Geração das chaves* - Nesta fase, o Centro Confiável gera as chaves secretas de cada usuário.

2. *Fase de assinatura* - Esta fase é dividida em duas etapas. O signatário, membro do grupo, prova para a Autoridade do Grupo sua identidade, e na seqüência, o signatário comprova o conhecimento da assinatura pelo grupo.

3. *Fase de verificação* - Supondo que o receptor conheça a identidade de cada membro do grupo, a assinatura pelo grupo pode ser verificada pelo receptor.

4. *Fase de identificação* - A Autoridade do Grupo pode identificar o signatário sem a ajuda dos membros individuais.

5. *Segurança* - A segurança do esquema é comprovada de forma que o seguinte seja mantido:

   I - Nenhum signatário pode forjar a assinatura de outro membro.

   II - Nem o receptor, nem mesmo a Autoridade do Grupo, pode gerar a assinatura em grupo.

   III - Nem o receptor, nem mesmo o Centro Confiável pode identificar o signatário da assinatura em grupo.

O esquema de Park, Kim e Won tem algumas limitações, no que diz respeito a inserção de novos elementos no grupo. Esse problema é tratado no artigo de Tseng e Jan [TSE 98]. As assinaturas prévias do grupo assinadas por outros membros será invalidada se o grupo se alterar. Em adição, o comprimento da assinatura em grupo é dependente do número de membros deste.

A proposta apresentada por Park, Kim e Won representa uma alternativa de uso das assinaturas em grupo, que faz uso da informação de identidade do membro para gerar as assinaturas pelo grupo. Uma segunda alternativa que se baseia na identidade é apresentada a seguir.

3.4 Um Novo Esquema de Assinaturas em Grupo com Base na Identidade

Como dito anteriormente, nas assinaturas em Grupo, membros individuais de um grupo podem fazer assinatura em favor do grupo. Entretanto, no caso de uma disputa futura, cada membro pode ser identificado pelos membros do grupo ou por uma autoridade, abrindo a assinatura para revelar a identidade do membro. Chaum e Heyst apresentaram quatro esquemas que satisfazem estas propriedades. Porém, as propostas de Chaum e Heyst possuem algumas limitações, como por exemplo, a necessidade de cada membro escolher uma nova chave, se o grupo for mudado. Esses esquemas foram aprimorados por Chen e Pedersen [CHE 94]. No entanto, os esquemas de assinaturas em grupo propostos continuam carentes de melhorias, principalmente por serem protocolos interativos e, conseqüentemente, ineficientes.

Outra limitação do esquema de Chen e Pedersen é apresentada a seguir. Quando a autoridade precisa verificar o membro da assinatura, deve anunciar alguma informação extra para verificar a identidade do assinante. Desta maneira, as assinaturas prévias podem ser identificadas pelo verificador ao mesmo tempo.

Em 1984, Shamir, conforme apresentado na Seção 4.2, introduziu a idéia de sistema de criptografia baseado em informação de identidade, tal como nome, endereço e descrição física [SHA 84]. Nesse sistema, a chave pública de cada entidade não é nada mais que a identificação que pode ser definida como parte da informação de identidade do elemento.

Em 1997, Park, Kim e Won apresentaram uma proposta que torna viável as assinaturas em grupo, usando a informação de identidade dos membros como base para geração das chaves públicas correspondentes [PAR 97].

Tseng e Jan apresentam um ligeiro avanço no esquema de criptografia baseado na identidade, propondo um novo esquema de assinaturas em grupo [TSE 98]. O esquema proposto preserva os principais méritos inerentes ao esquema de assinaturas em grupo baseado na identidade, proposto por Park, Kim e Won, especialmente pelo fato

de que a chave pública de cada entidade será a própria identidade do signatário. Além disso, o esquema proposto resolve problemas de invalidação de assinaturas prévias pela inclusão ou exclusão de um membro no grupo, e o comprimento da assinatura em grupo possui um tamanho fixo.

Esta seção é apresentada pelas subseções a seguir. Na Subseção 3.4.1 o esquema de Assinaturas em Grupo proposto por Tseng e Jan é apresentado. Na Subseção 3.4.2 faz-se as considerações de segurança da proposta de Tseng e Jan. Finalmente, na Subseção 3.4.3 faz-se algumas comparações entre os esquemas de Assinaturas em Grupo com base na identidade, apresentados neste capítulo.

3.4.1 O Esquema de Assinaturas em Grupo Proposto por Tseng e Jan

O esquema proposto por Tseng e Jan é dividido em três estágios, a saber, o estágio de *Inicialização*, *Assinaturas em Grupo e Verificação* e *Identificação de Usuário*, a seguir descritos [TSE 98]:

1. *Inicialização* - Este estágio consiste em duas fases, a fase de *inicialização do sistema* e a fase de *criação de grupo*, a seguir descritas:

   - *Inicialização do sistema* - Esta fase consiste na geração e distribuição da chave secreta K_{T_i}. Supõe-se que um usuário de um sistema aberto de comunicação de dados, U_i, cuja informação de identidade correspondente é ID_i, queira participar do esquema de assinaturas em grupo. A primeira etapa do processo consiste na geração de uma chave secreta K_{T_i} pela **Autoridade Confiável**, T, e posterior envio para o usuário U_i, por um canal seguro. O cálculo da chave K_{T_i} é feito em função da informação de identidade ID_i, que corresponde à chave pública do usuário U_i.

   - *Fase de Criação de Grupo* - Um segundo elemento confiável, denominado **Autoridade do Grupo**, GA, é responsável pela geração e distribuição de uma

segunda chave secreta, K_{GA_i}, calculada em função da informação de identidade ID_i e da chave assimétrica secreta da Autoridade do Grupo KR_{GA}. Para cada membro do grupo U_i, cuja identidade é ID_i, a Autoridade do Grupo gera a chave secreta K_{GA_i} e envia para U_i, por um canal seguro, juntamente com sua chave assimétrica pública KU_{GA}.

2. *Assinatura em Grupo e Verificação* - Suponha que um usuário U_i queira assinar uma mensagem M. As assinaturas em grupo são obtidas com um processo assinatura que faz uso das duas chaves secretas, K_{T_i} e K_{GA_i}.

   Em possuindo a chave pública KU_{GA}, qualquer usuário, U_i, poderá verificar as assinaturas em grupo, certificando se as assinaturas foram realmente geradas por elementos do grupo. Porém, esse usuário, denominado *elemento verificador*, não conseguirá identificar qual dos elementos do grupo assinou a mensagem M.

3. *Identificação do Usuário* - No caso de disputa, a assinatura em grupo pode ser aberta de maneira a identificar o signatário da mensagem, revelando sua identidade, ID_i. A Autoridade de Grupo, fazendo uso da chave secreta KR_{GA}, pode identificar o signatário sem a necessidade de assistência dos membros do grupo para achar ID_i.

   Em ordem, para convencer outros elementos do grupo que o usuário U_i, com identidade ID_i, é o signatário, a Autoridade do Grupo publica a informação de identidade do usuário ID_i por um canal seguro. Ao receber a informação da Autoridade do Grupo, o elemento verificador pode identificar a identidade ID_i do signatário.

   Uma outra característica consiste em que, mesmo a Autoridade de Grupo anunciando a chave ID_i, não haverá necessidade de renovar a chave do signatário. A razão é que a informação é apenas fornecida para a assinatura pelo grupo específica e para a mensagem M. O anonimato do signatário em questão, relativamente a qualquer outra assinatura anterior ou de futuras assinaturas, não é quebrado.

3.4.2 Análise de Segurança do Esquema de Tseng e Jan

Quatro ataques possíveis contra o esquema proposto por Tseng e Jan são apresentados. O ataque 1 apresenta um adversário malicioso tentando achar a chave assimétrica secreta da Autoridade do Grupo, KR_{GA}. Os ataques 2 e 3 são feitos por elementos que buscam forjar as assinaturas em grupo e o ataque 4 é feito para tentar quebrar o anonimato do usuário. Apresenta-se a seguir o comportamento do protocolo proposto por Tseng e Jan mediante esses ataques.

- *Ataque 1* - Um adversário tenta descobrir a chave secreta da Autoridade do Grupo, KR_{GA}, a partir da sua chave pública KU_{GA}, e dos anúncios prévios. Nas aproximações descritas, entretanto, ele vai se deparar com a dificuldade de calcular o módulo logaritmo discreto do número composto N, o que é tão ou mais difícil que fatorar os módulos.

- *Ataque 2* - Qualquer membro do grupo, U_i, ou mesmo um adversário malicioso que não é membro do grupo, representados por Melo, podem tentar forjar uma assinatura pelo grupo. Considerando que somente o usuário, U_i, e a Autoridade do Grupo, GA, conhecem a chave secreta K_{GA_i}, Melo não poderá gerar uma assinatura pelo grupo válida. Para obter a chave válida K_{GA_i}, Melo necessita revelar a chave assimétrica secreta da Autoridade do Grupo, KR_{GA}, e então calcular K_{GA_i}. Para que isso seja possível, tal como no ataque 1, Melo irá se deparar com o cálculo do módulo logaritmo discreto para o número composto N.

- *Ataque 3* - Nesse caso, supõe-se a Autoridade do Grupo ou um adversário malicioso, Melo, sem o conhecimento da chave secreta K_{T_i} do usuário U_i, tenta personificar U_i e forjar a assinatura pelo grupo. Embora a Autoridade do Grupo conheça a chave secreta K_{GA_i} de cada membro do grupo U_i, ela não pode forjar uma assinatura no grupo com a identidade de U_i, pois não conhece K_{T_i}. A complexidade computacional para se obter K_{T_i} a partir de ID_i ou de assinaturas prévias de U_i é tão difícil quanto o cálculo do módulo logaritmo discreto para um número composto N. Conseqüentemente, se nem mesmo a Autoridade do Grupo não consegue

personificar U_i e forjar a assinatura pelo grupo, para Melo será ainda mais difícil alcançar esse intento.

- *Ataque 4* - Um receptor tenta determinar a identidade do signatário da assinatura pelo grupo. Cada membro do grupo pode assinar uma mensagem em favor do grupo sem revelar sua identidade. Apenas a Autoridade do Grupo é capaz de revelar a identidade do assinante. Desde que o receptor não conheça a chave assimétrica secreta da Autoridade do Grupo, KR_{GA}, ele não poderá determinar ID_i. Como analisado no ataque 1, obter KR_{GA} implica que ele irá se deparar com o cálculo do módulo logaritmo discreto para o número composto N.

3.4.3 Comparação do Esquema de Tseng e Jan com o de Park, Kim e Won

O esquema de assinaturas em grupo de Tseng e Jan apresenta algumas melhorias em relação ao esquema proposto por Park, Kim e Won [PAR 97].

No esquema proposto por Park, Kim e Won, cada membro calcula a assinatura pelo grupo de acordo com sua chave secreta e as identidades de todos os membros do grupo. Entretanto, para assinar a mensagem em favor do grupo, cada assinante precisa saber tudo das identidades dos membros do grupo. Além disso, o receptor deve saber tudo das identidades dos membros do grupo para verificar a assinatura pelo grupo. Por esta razão, se o grupo mudar, as assinaturas que usavam as identidades prévias dos membros do grupo serão inválidas. Ainda, o tamanho da assinatura do grupo é linearmente proporcional ao tamanho do grupo.

Os problemas acima relacionados não aparecem na proposta de Tseng e Jan, que permite a inclusão de novos membros, sem que as assinaturas prévias sejam invalidadas. Em adição, o tamanho da assinatura pelo grupo é independente do tamanho do grupo.

3.5 Conclusão

As técnicas acima apresentadas, sobre Assinaturas em Grupo, viabilizam uma comunicação entre um grupo de usuários de um sistema aberto de comunicação de dados, com algumas características especiais. A questão do anonimato também é constantemente tratada. O que se busca com esta pesquisa é identificar características e funcionalidades que possam servir como solução para o problema da comunicação anônima segura em grupo.

Verificou-se que as assinaturas em grupo se relacionam bastante com o tema deste trabalho de pesquisa. Porém, as características das assinaturas em grupo, tal como apresentadas na literatura, não são suficientes para viabilizar uma comunicação anônima segura entre um grupo de usuários, que atenda as necessidades descritas na Seção 1.3. O que se busca é uma alternativa de comunicação que torne viável a garantia incondicional do anonimato do emissor, exceto para o receptor, para quem a mensagem é direcionada.

Nas assinaturas em grupo, o anonimato do emissor ou signatário pode ser quebrado, a qualquer momento, por uma Autoridade genérica. O que se busca com esta pesquisa é que o anonimato do emissor não possa ser quebrado em hipótese nenhuma, nem mesmo por uma Autoridade. O único elemento que será capaz de identificar a origem da mensagem é o receptor, e nem mesmo ele poderá comprovar a identidade do emissor para um terceiro.

Capítulo 4

Esquemas de Identificação

Fez-se, nos capítulos anteriores, além de uma revisão teórica sobre diversos assuntos da criptografia, uma minuciosa pesquisa, com o objetivo de encontrarmos algumas características específicas que possam nos auxiliar na elaboração de uma proposta, cujo objetivo é resolver o problema da comunicação anônima segura em grupo, apresentado na Seção 1.2.

As assinaturas em grupo, estudadas no Capítulo 3, representam uma alternativa de aplicação que viabiliza uma comunicação entre um grupo restrito de usuários de um sistema aberto de comunicação de dados, com características bastante específicas. Para a proposta dessa pesquisa, as assinaturas em grupo representam a aplicação que mais se relaciona com o tema Comunicação Anônima Segura em Grupo. Porém, dentre as alternativas sugeridas na literatura, não se identificou nenhuma que pudesse ser diretamente aplicada como uma solução para o problema apresentado.

Uma vez que não se tem uma solução imediata para o problema da comunicação anônima segura em grupo, para a continuidade dessa pesquisa, faz-se necessário um estudo mais específico e que mais se aproxime da raiz do problema.

Para se conseguir uma comunicação anônima segura em grupo, em consonância com a necessidade apresentada na Seção 1.3, faz-se necessário que o elemento receptor, Beto, consiga identificar a origem específica da mensagem M, ou seja, consiga saber a identidade do emissor, Alice, sem que Beto tenha como revelar isso a um terceiro.

O tema da criptografia que estuda as maneiras que Beto tem para identificar Alice é denominado *esquemas de identificação*. Os esquemas de identificação são objetos de estudo deste capítulo, que é dividido nas seguintes seções:

Na Seção 4.1, o conceito de esquemas de identificação é introduzido. Na Seção 4.2, introduz-se o conceito de esquemas de assinatura digital com base na identidade, ID. Na Seção 4.3, apresenta-se uma alternativa de implementação dos esquemas de identificação com base na prova de conhecimento-zero. Na Seção 4.4, apresenta-se uma alternativa baseada na dificuldade de solução do módulo logaritmo discreto. Na Seção 4.5, discute-se um tipo de esquemas de identificação com base no limiar. Na Seção 4.6, apresenta-se uma proposta de comunicação destinada a difusão segura para um grupo arbitrário de receptores. Finalmente, na Seção 4.7 faz-se as considerações finais desse capítulo.

4.1 Introdução a Esquemas de Identificação

Em aplicações que usam um sistema aberto de comunicação de dados, constantemente, faz-se necessário que usuários desse sistema identifiquem uns aos outros. Os esquemas de identificação tornam viável que os usuários de um sistema aberto de comunicação de dados possam identificar uns aos outros, atribuindo uma identidade, ID, a cada usuário.

Aplicações típicas de esquemas de identificação incluem passaportes, cartões de crédito, senhas de computadores, ordens militares e, sistemas de controle, nos quais existe a necessidade de se identificar a identidade do usuário, ID. Os esquemas de identificação podem vir a ser a base para um novo tipo de identificação pessoal, com a qual poder-se-á assinar cheques digitalmente, bilhetes de cartão de crédito, documentos legais e correio eletrônico.

Laith e Chen definem *esquemas de identificação* da seguinte maneira [LAI 91]:

> ”Um esquema de identificação permite a um elemento A provar sua identidade, ID, para outro usuário B através de um canal aberto de comunicação de dados.

Ninguém, incluindo B, pode provar para um terceiro a identidade de A."

Para ser útil e seguro, um esquema de identificação deve satisfazer as seguintes três condições:

- A probabilidade de um verificador real aceitar uma prova verdadeira de identidade deve ser extremamente alta.
- A probabilidade de um verificador real aceitar uma prova falsa de identidade deve ser extremamente pequena.
- Um verificador trapaceiro não deve aprender nada relativo às funções do verificador real. As chances de um verificador trapaceiro se passar por um verificador real deve ser extremamente pequena.

Analogamente à classificação de protocolos criptográficos interativos, apresentada na Seção 2.11, os esquemas de identificação também podem ser classificados como interativos, mediante a necessidade de interações para que o receptor B possa identificar o emissor A. Uma análise da segurança de esquemas de identificação interativos é apresentada por Shoup [SHO 96].

Uma outra definição de esquemas de identificação é apresentada por Kim e Kim, a seguir descrita [KIM 02]:

"Um esquema de identificação é um protocolo interativo, onde um elemento comprovador A tenta convencer um elemento verificador B sobre sua identidade."

Em linhas gerais, um esquema de identificação é dito quebrado se um adversário não autorizado personificar A, fazendo com que B aceite a prova de maneira indevida. Os ataques são classificados de acordo com a interação permitida ao adversário antes da tentativa de personificação. São duas as formas básicas de ataques:

- *Ataque Passivo* - É a maneira mais frágil de ataque, onde o adversário não tem permissão para interagir com o sistema antes da tentativa de personificação. A única informação disponível para o adversário é a chave pública de A.

- *Ataque Ativo* - É a maneira mais forte de ataque, onde é permitido ao adversário uma série de interações com o emissor A, colocando-se como sendo o receptor B.

Kim e Kim complementam da seguinte forma: apenas A sabe o valor secreto correspondente ao seu valor público, e este valor secreto o habilita a convencer B sobre sua identidade. Ao se trocar a palavra *identidade* por *autenticidade* de uma mensagem, os esquemas de identificação se equivalem a *esquemas de assinatura*, sendo a diferença entre ambos bastante sutil.

Como visto, os esquemas de identificação se assemelham bastante com os esquemas de assinatura digital, objeto de estudo da Seção 2.6. Faz-se a seguir, na Subseção 4.1.1, um comparativo entre esquemas de identificação e de assinatura digital.

4.1.1 Comparativo entre Esquemas de Identificação e de Assinatura Digital

Informalmente, pode-se definir assinatura digital como sendo um valor associado, fácil de comprovar e difícil de forjar. Após tendo sido gerada e verificada a assinatura, ela pode ser apresentada a um juiz, de maneira que o signatário não pode negar a autoria da mensagem.

Um esquema de identificação é uma assinatura simplificada na qual não existe disputa de mensagens ou juízes: a prova da identidade é interativa, e o verificador pode facilmente aceitar ou rejeitar a prova da identidade, sem nenhuma conseqüência legal ou cobrança futura [MIC 88].

Para melhor compreensão da diferença entre esquemas de identificação e de assinatura digital, apresenta-se uma citação onde Schneier escreve a respeito da conversão de um esquema de identificação em assinatura digital [SCH 96a]:

> ”Existe um método padrão para converter um esquema de identificação em um esquema de assinatura: realimentando o elemento verificador com um resumo da mensagem. A mensagem não tem uma função resumo até que seja assinada, e isto pode ser feito ao invés de gerar a função no algoritmo de assinatura. Em princípio, isto pode ser feito com qualquer esquema de identificação.”

O resumo da mensagem $H(M)$ é o fator que garante a integridade da mensagem M, e o não-reuso da assinatura. Sendo assim, considerando esta citação de Schneier conclui-se: os esquemas de identificação são suficientes para os usuários de um sistema aberto de comunicação de dados se identificarem. Porém, os esquemas de identificação não garantem a integridade e a autenticidade das mensagens trocadas. Essas garantias só podem ser obtidas com os esquemas de assinatura digital.

Fiat e Shamir também fazem uma comparação entre os esquemas de identificação e de assinatura digital [FIA 86]. Um terceiro tipo de esquema ainda é objeto desta comparação, o de autenticação, a seguir apresentada:

- *Esquemas de Identificação* - Alice pode provar para Beto que ela é realmente Alice. Beto não pode provar a ninguém mais que ela é Alice.

- *Esquemas de Assinatura* - Alice pode provar para Beto que ela é Alice. A identidade de Alice fica associada à mensagem M emitida, sendo que, ninguém, nem mesmo Beto, tem como dizer que é o emissor da mensagem assinada.

- *Esquemas de Autenticação* - Alice pode provar para Beto que ela é realmente Alice. Ninguém pode provar para Beto que ela é Alice, senão ela mesma.

A Figura 4.1 ilustra a diferença entre os esquemas acima relacionados. A *autenticação* consiste em Beto conseguir saber se Alice é realmente quem ela está dizendo ser, sendo que somente Alice pode provar sua própria identidade. A *identificação* consiste em Alice provar sua identidade para Beto, sendo que Beto não pode comprovar a identidade de Alice a um terceiro elemento. A *assinatura* consiste em Alice provar sua identidade para Beto, e qualquer outro elemento pode verificar a identidade como sendo de Alice.

Esquemas de autenticação são úteis apenas contra ameaças externas, quando Alice e Beto interagem. A distinção entre esquemas de identificação e esquemas de assinatura se manifesta principalmente quando a prova é interativa e o verificador posteriormente deseja provar sua existência a um juiz.

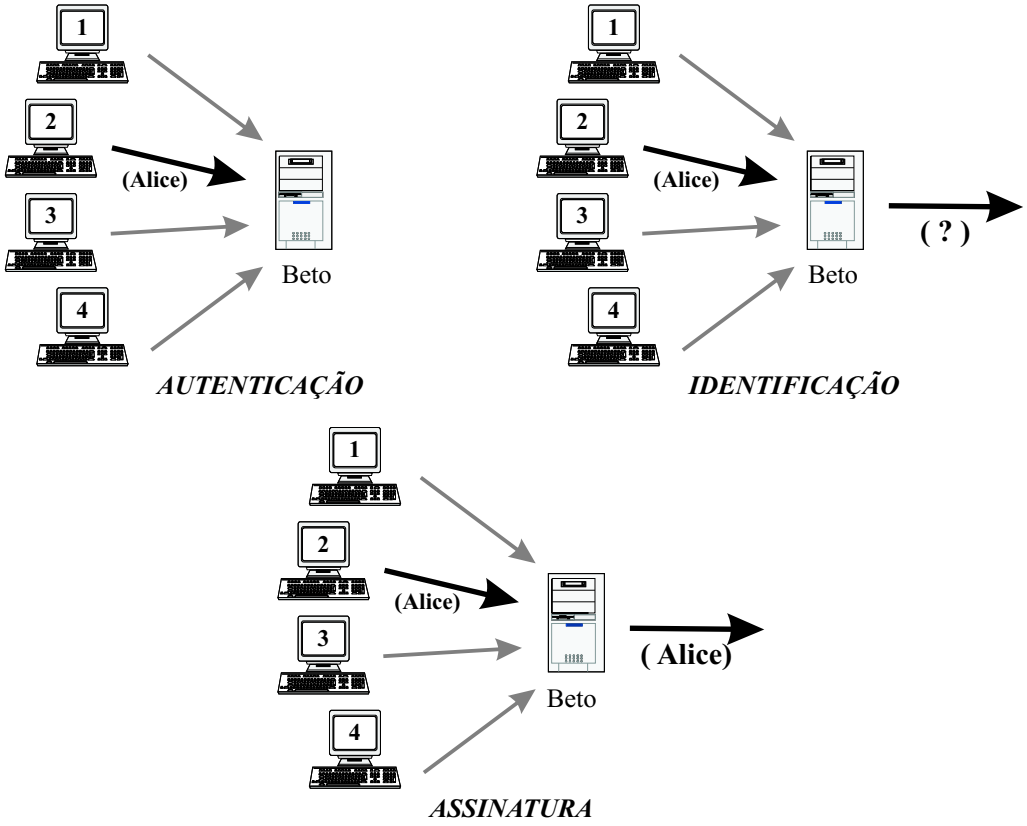

Figura 4.1: Ilustração dos Esquemas de Autenticação, Identificação e Assinatura - Essa figura ilustra a diferença entre os esquemas de autenticação, identificação e assinatura digital.

4.2 Esquemas de Assinatura Baseados na Identidade

Shamir introduziu um novo tipo de esquema criptográfico, que habilita qualquer par de usuários a se comunicarem de forma segura e verificarem as assinaturas sem a troca de chaves privadas ou públicas, sem manterem diretórios de chaves e sem usarem serviços de um terceiro elemento [SHA 84]. O esquema assume a existência de centros confiáveis de geração de chaves, cujo propósito único será dar a cada usuário um cartão inteligente personalizado (*Smart Card*) no momento que ele se associar à rede pela primeira vez. A informação embutida nesse cartão habilitará o usuário a assinar e cifrar as mensagens que ele enviará, e decifrar e verificar as mensagens que ele receber de maneira totalmente independente, sem levar em consideração a identidade da outra parte.

Inicialmente os cartões fabricados não terão que ser atualizados quando novos usuários se integrarem à rede, e os vários centros não precisarão coordenar suas atividades para manter a lista de usuários. Não haverá mais necessidade dos centros após a emissão dos cartões, e a rede pode continuar a operar de maneira totalmente descentralizada por um período indefinido.

O esquema de Shamir é ideal para grupos fechados de usuários, tais como executivos de uma companhia multinacional, ou ramificações de um grande banco, desde que os quartéis-generais da corporação possam servir como um centro de geração de chaves que todos confiam.

O conceito é fundamentado em um sistema criptográfico de chaves públicas, com um adendo: ao invés de gerar um par randômico de chaves assimétricas secretas e publicar uma das chaves, o usuário escolhe seu nome, endereço de rede e chave pública. Qualquer combinação de nome, CPF, endereço, escritório e número telefônico pode ser usado, dependendo do contexto, provendo uma identidade única que o usuário não poderá posteriormente negar, e que estará prontamente disponível para a outra parte. A chave secreta correspondente será gerada por um Centro de Geração de Chaves e emitida para o usuário em forma de um cartão inteligente, no instante que o usuário se ligar à rede pela primeira vez. O cartão contém processador, dispositivos de entrada e saída, memória volátil (*Random Access Memory - RAM*), memória não volátil (*Read Only Memory - ROM*) com a chave secreta, e programas para cifrar e decifrar mensagens, gerar e verificar as assinaturas.

Um esquema de assinatura digital baseado na identidade, ID, se assemelha a um sistema de mensagens ideal: caso se conheça o nome e endereço de Beto poder-se-á enviar mensagens para ele, de maneira que somente ele poderá ler, e poder-se-á verificar a assinatura que somente Beto poderia ter produzido. Isto faz o aspecto criptográfico da comunicação quase transparente ao usuário, e pode ser usado, efetivamente, mesmo por leigos que não sabem nada sobre chaves ou protocolos.

Quando um usuário A quer enviar uma mensagem para B, ele assina a mensagem com a chave secreta de seu cartão eletrônico, cifra o resultado usando a identidade de B (nome e endereço de rede), adiciona sua própria identidade e envia para

B. Quando B recebe a mensagem, ele decifra usando a chave secreta de seu cartão eletrônico, e então verifica a assinatura, usando a identidade do emissor como uma chave de verificação.

A chave secreta pode ser gerada por um Centro de Geração de Chaves ao invés dos usuários, desde que não haja nada especial com a identidade deles: se A pode gerar a chave secreta que corresponde à chave pública de A, ele pode também gerar as chaves secretas correspondentes a B, C etc., e o esquema não será seguro. O Centro de Geração de Chaves deve estar em uma posição privilegiada por saber algumas informações secretas, que o habilita a gerar as chaves secretas de todos usuários da rede.

Um sistema criptográfico baseado na identidade está representado na Figura 4.2. Nos esquemas baseados na identidade, a chave usada para cifrar é a identi-

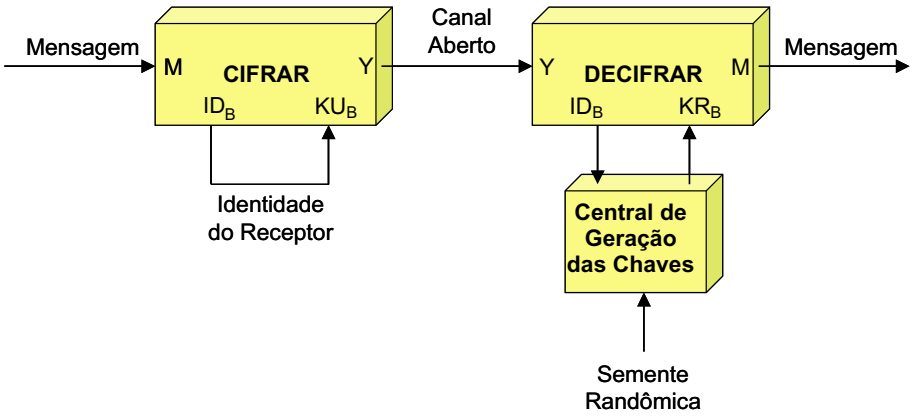

Figura 4.2: Estrutura do Sistema Criptográfico Baseado na Identidade - Nessa estrutura, a chave pública KU é gerada única e exclusivamente em função da identidade do elemento que possui a chave privada KR.

dade do receptor ID_B, ou seja $KU_B = ID_B$, e a chave usada para decifrar é derivada da identidade ID_B e da semente randômica, K, ou seja $KR_B = f(ID_B, K)$. O canal seguro entre os usuários, necessário nos sistemas criptográficos de chaves simétricas e assimétrica, é eliminado por completo, e é substituído por uma interação única com o Centro de Geração de Chaves, no momento que o receptor participa do sistema pela primeira vez.

Os conceitos acima descritos representam uma alternativa bastante interessante de um elemento emissor, A, se identificar perante um elemento receptor, B,

ou seja, A pode usar sua própria identidade, ID_A, para se identificar de maneira segura. Possibilitou-se, então, o desenvolvimento de um esquema de assinatura digital baseado na identidade.

Analogamente, o esquema de assinatura baseado na identidade é bastante semelhante ao esquema baseado em chaves assimétricas, porém não há necessidade do diretório público. A Figura 4.3 ilustra esse processo. A diferença é que a chave KU_A é

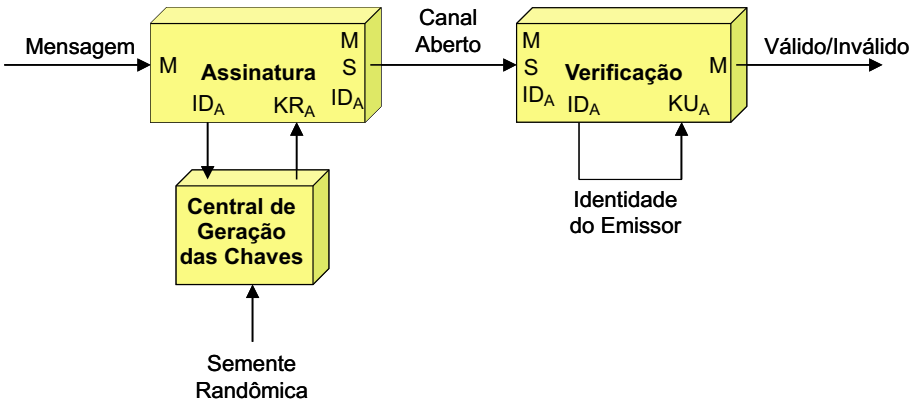

Figura 4.3: Estrutura do Esquema de Assinatura Baseado na Identidade - No esquema de assinatura baseado na identidade a chave KU_A é gerada em função da identidade do emissor, e a chave KR_A é gerada em função da identidade do emissor e de uma semente randômica, K.

gerada em função da identidade do emissor, e a chave KR_A é gerada em função da identidade do emissor e de uma semente randômica, K. A mensagem M, juntamente com a assinatura S e a identidade ID_A é transmitida pelo canal aberto de comunicação.

4.3 Prova de Identidade Usando a Prova de Conhecimento-Zero

Nessa seção, apresenta-se uma outra alternativa que torna viável a prova de identidade, usando a prova de conhecimento-zero.

O uso da prova do conhecimento-zero, como uma ferramenta de prova da identidade, foi inicialmente proposto por Fiat e Shamir [FIA 86]. Eles descrevem

um esquema de identificação e assinatura que habilitam qualquer usuário a comprovar sua identidade e a autenticidade de sua mensagem para qualquer outro usuário, sem compartilhar ou publicar chaves criptográficas. Este esquema é baseado na *Prova de Conhecimento-Zero* [GOL 85], usada especificamente para identificação. No esquema proposto por Fiat e Shamir, a chave privada do emissor, KR_A, é uma função da sua identidade ID_A, $KR_A = f(ID_A)$. Usando a prova do conhecimento-zero, Alice prova que conhece sua chave privada KR_A, e, conseqüentemente, prova sua identidade ID_A.

A Prova de Conhecimento-Zero, apresentada na Seção 2.9, pode ser feita com intuito de verificar a identidade de um elemento qualquer na rede. Feige, Fiat e Shamir modificaram o esquema inicialmente proposto por Fiat e Shamir criando a prova de identidade de conhecimento-zero, em [FEI 87] e [FEI 88].

Schneier descreve o esquema de identificação de Feige, Fiat e Shamir de forma simplificada [SCH 96a]. Antes de lançar mão das chaves privadas, uma Autoridade Confiável escolhe um número aleatório n, sendo n resultado do produto de dois números primos grandes o bastante. No mundo real, n tem que ser pelo menos um número de 512 bits. Esse n pode ser distribuído entre um grupo de elementos que, posteriormente, irão identificar a identidade do emissor, ou *elementos verificadores*. Para gerar as chaves pública e privada, a Autoridade Confiável escolhe um número v, onde v é um resíduo quadrático mod n, ou seja, escolhe v tal que $x^2 = v$ mod n tem solução e v^{-1} mod n existe. Esse valor v é a chave pública de Alice, KU_A. Então, calculando o menor valor de s tal que $s = \sqrt{v^{-1}}$ mod n, define-se s como a chave privada de Alice, KR_A. Considere que Alice queira comprovar sua identidade para Beto. O protocolo de identificação pode agora prosseguir assim:

1. Alice escolhe um número randômico r, sendo r menor que n. Então Alice calcula $x = r^2$ mod n, e envia x para Beto.

2. Beto envia para Alice um número aleatório b, sendo $b = 0$ ou 1.

3. Se $b = 0$, Alice envia para Beto r. Se $b = 1$, Alice envia para Beto $y = r \times s$ mod n.

4. Se $b = 0$, Beto verifica que $x = r^2$ mod n, provando que Alice conhece $\sqrt{x}$. Se $b = 1$, Beto verifica $x = y^2 \times v$ mod n, comprovando que Alice conhece $\sqrt{v^{-1}}$.

Este é o ciclo do protocolo denominado *credenciamento*. Alice e Beto podem repetir esse ciclo várias vezes, até que Beto se convença de que Alice conhece s, que é a chave privada de Alice, KR_A, ou seja, são necessárias várias interações para que Beto esteja convencido da identidade de Alice.

4.4 Esquemas de Identificação com Base no Logaritmo Discreto

Schnorr demonstra uma nova alternativa de implementação, apresentando um esquema de identificação interativo baseado no logaritmo discreto, destinado a cartões inteligentes [SCH 89]. O esquema proposto minimiza o trabalho a ser feito pelo cartão inteligente para gerar uma assinatura e provar sua identidade, uma vez que a capacidade de processamento do cartão inteligente é bastante limitada. Os esquemas de assinatura propostos, até então, para implementação em cartões inteligentes requerem várias multiplicações modulares para gerar a assinatura. Na proposta de Schnorr, o esquema de geração de assinatura custa em torno de 12 multiplicações modulares, independentes da mensagem e da identificação, o que pode ser feito durante o tempo livre do processador. A segurança do esquema permanece e é baseada na dificuldade de solução do logaritmo discreto.

Schnorr apresenta outra proposta de implementação dos esquemas de identificação, onde se faz melhorias na proposta de Fiat e Shamir [FIA 86], tornando as interações mais rápidas, obtendo um esquema de assinatura bastante eficiente [SCH 96b].

Okamoto também apresenta três propostas de implementação dos esquemas de identificação e esquemas de assinatura digital correspondentes, baseados na dificuldade de solução do módulo logaritmo discreto [OKA 92].

4.5 Identificação Pelo Limiar

Existem situações mais específicas onde os esquemas de identificação apresentados nesse capítulo, até então, não são apropriados. Em muitas aplicações é preciso identificar a organização acima da identidade individual dos membros. Um esquema de identificação pelo limiar é um esquema onde a identificação do grupo poderá ser feita se n dos m membros do grupo concordam em comprovar sua identidade de forma anônima.

Laith e Chen ampliaram o conceito de identificação de usuário para a identificação no limiar, com objetivo de provar a identidade do grupo [LAI 91]. Um esquema de identificação pelo limiar é um esquema em que a prova da identidade do grupo pode ser identificada por alguém, se n membros de um grupo de m componentes concordam em comprovar a identidade do grupo. De maneira geral, existem dois métodos para satisfazer esta necessidade, a seguir descritos.

- **Método 1 -** Cada grupo é visto como um usuário e tem uma chave secreta. O Centro de Geração de Chaves distribui as chaves secretas do grupo para cada membro individual, secretamente.

  Identificação - Tal como nos esquemas de identificação de Fiat-Shamir ou Schnorr, um verificador identificará cada membro individualmente. Se o número de membros que participam do protocolo for maior que n, o verificador aceitará a prova da identidade do grupo. Caso contrário, a prova será rejeitada.

- **Método 2 -** Cada grupo é visto como um usuário e tem uma chave secreta. O Centro de Geração de Chaves divide o segredo em partes, tal que o seguinte se mantenha:

  (a) Qualquer união de n partes pode reconstituir o segredo.

  (b) O conhecimento de $n-1$ ou menos partes não contém informação nenhuma sobre o segredo.

  Em seguida, o Centro de Geração de Chaves distribuirá as partes secretamente para os membros do grupo.

Identificação - Neste método, n membros necessitam se unir para reconstruir a chave secreta do grupo. Tal como nos esquemas de identificação de Fiat-Shamir ou Schnorr, o verificador identificará a representação dos n membros. Se cada representação passar pela verificação, então a identidade do grupo será aceita, ou, caso contrário, será rejeitada.

O método 1 falhará se qualquer dos membros dividir seu segredo com $n-1$ pessoas de fora do grupo. Além disso, será impossível identificar qual é o membro traidor.

O método 2 também falhará, uma vez que os representantes poderão manter a chave secreta do grupo para uma próxima identificação.

O protocolo de identificação baseado no limiar permitirá a prova de identidade do grupo por qualquer membro da rede, se os membro do grupo que concordarem em provar sua identidade de maneira anônima for maior que o valor de limiar n. No protocolo proposto por Laith e Chen, o elemento verificador identifica os n membros do grupo individualmente, de acordo com o Método 1 descrito acima.

4.6 Transmissão Segura por Difusão

Um outro tipo de esquema, que torna viável uma transmissão segura por difusão, é apresentado nesse capítulo. O objetivo desse esquema é possibilitar um Centro de Distribuição fazer uma transmissão segura para um grupo arbitrário de receptores, minimizando os problemas de gerenciamento das chaves para uma transmissão desse tipo.

Suponha um esquema que permita a um Centro de Distribuição transmitir uma mensagem M para qualquer subgrupo de usuários privilegiados, pertencentes a um universo finito de m, de maneira que k usuários não têm privilégio e não podem descobrir o segredo. A questão principal é que o Centro de Distribuição deseja fazer uma transmissão para o subgrupo dinâmico de usuários que possuem o privilégio, de maneira que os membros que não possuem o privilégio não possam ter acesso à mensagem. Naturalmente, alguns membros sem privilégios poderão ficar curiosos sobre o conteúdo da

mensagem M que está sendo difundida, e poderão tentar decifrá-la de qualquer maneira. A transmissão segura por difusão busca impedir que esse tipo de problema ocorra.

Uma primeira alternativa é imediata e consiste em cada usuário, como por exemplo A, B e E, possuir sua própria chave secreta, KU_A, KU_B e KU_E, respectivamente. O Centro de Distribuição transmitirá as mensagens M cifradas individualmente para cada membro que possui o privilégio. Isso irá requerer uma transmissão para cada elemento, caracterizando uma transmissão muito longa. Essa primeira alternativa é ilustrada na Figura 4.4.

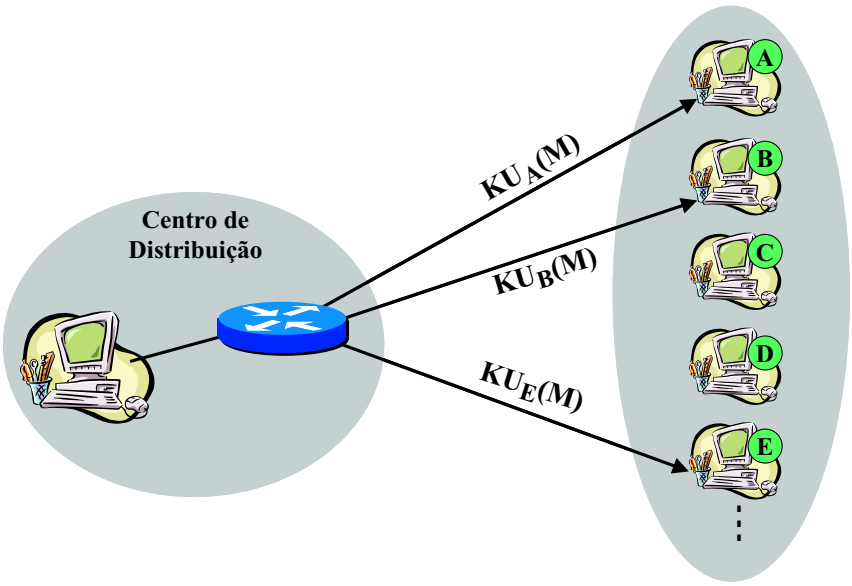

Figura 4.4: Esquema de Difusão por Transmissão Direta - A primeira maneira para se fazer distribuição da mensagem para um subgrupo de usuários, de maneira direta, cifrando as mensagens e transmitindo-as individualmente para cada elemento.

A Figura 4.5 ilustra uma segunda alternativa. Essa segunda alternativa de solução consiste em prover cada subgrupo possível de um único par de chaves pública e privada correspondente. Isso iria demandar que cada usuário armazenasse um número significativo de chaves, diretamente proporcional ao dobro das quantidades possíveis de subgrupos. Esta solução consiste em cada subgrupo possuir uma chave única, de maneira que a mensagem para um subgrupo é enviada uma única vez. Na figura, considera-se que a chave $G1$ é de conhecimento de A, B e E. Nesse processo, a mensagem M é enviada pelo

Centro de Distribuição para o subgrupo uma única vez, codificada com a chave pública do subgrupo, para todos os elementos do grupo. Porém, somente quem possui a chave privada do subgrupo específico conseguirá decifrar a mensagem. O problema com essa

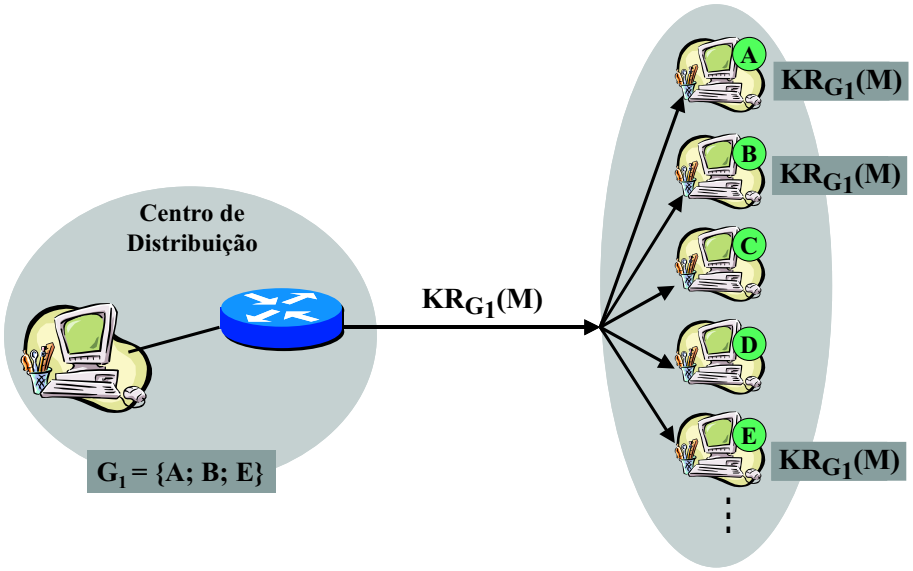

Figura 4.5: Esquema de Difusão Por Subgrupo - Essa solução consiste em cada subgrupo possuir um chave única. A mensagem para um subgrupo é enviada uma única vez.

solução é que cada usuário poderá possuir uma quantidade enorme de chaves, uma vez que um usuário poderá pertencer a vários subgrupos.

Na primeira solução, o problema é o tamanho da transmissão. Na segunda solução, é a necessidade de armazenar localmente nos usuários uma quantidade potencialmente grande de pares de chaves públicas e privadas, relativas a cada subgrupo que o usuário faça parte.

Um esquema alternativo, destinado para transmissão em difusão, foi proposto por Fiat e Naor [FIA 98]. O objetivo do esquema de Fiat e Naor é prover uma solução eficiente para ambos os casos acima apresentados. Ou seja, visa minimizar tanto o tamanho da transmissão quanto o espaço de armazenamento nos usuários finais, objetivando ainda a construção de um esquema computacionalmente eficiente.

4.7 Conclusão

Os esquemas de identificação, objeto de estudo desse capítulo, tratam as maneiras que um elemento emissor, Alice, tem para comprovar sua identidade para um elemento receptor, Beto. Para eliminar as confusões que por ventura possam ocorrer entre esquemas de identificação e de assinatura digital, fez os devidos esclarecimentos.

Apresentou-se, então, uma pesquisa das diversas propostas de esquemas de identificação, na busca de uma alternativa que se enquadre como uma solução para o problema da comunicação anônima segura em grupo.

O que se busca com essa pesquisa é um esquema de identificação que torne viável para um emissor, Alice, se identificar perante um receptor, Beto. Um esquema de assinatura correspondente também deve ser apresentado, possibilitando que Alice envie mensagens seguras e confidenciais para Beto, que, por sua vez, não poderá revelar a identidade de Alice para um terceiro.

Nenhuma das propostas estudadas seriam suficientes para a solução imediata do problema da comunicação anônima segura em grupo, porém, as características estudadas, neste capítulo, são de enorme importância para consubstanciar o protocolo proposto no Capítulo 5.

Capítulo 5

Protocolo Proposto

Descreve-se neste capítulo, detalhadamente, um protocolo criptográfico para comunicação anônima segura em grupo, que representa uma alternativa de solução do problema, foco dessa pesquisa, apresentado na Seção 1.2.

Para representação ilustrativa do protocolo, utiliza-se a seguinte notação gráfica:

- Cada elemento que participa do esquema proposto será representado por figuras com respectivos nomes.
- As linhas tracejadas representam a troca de chaves.
- As linhas cheias representam a troca efetiva de informação.
- Os números entre círculo representam os passos a serem seguidos para descrição do protocolo.

As seções desse capítulo foram divididas conforme apresentado a seguir.

Inicialmente, faz-se uma contextualização do problema a ser resolvido, na Seção 5.1. A proposta de solução a ser apresentada é discutida na Seção 5.2. Apresenta-se então, na Seção 5.3, uma descrição detalhada do protocolo proposto, capaz de tornar viável uma comunicação anônima segura em grupo, demonstrando cada passo a ser seguido no protocolo. Na Seção 5.4, faz-se as considerações sobre o funcionamento do

protocolo. Na Seção 5.5 faz-se a extensão do conceito apresentado para comunicação em grupo. As considerações finais são apresentadas na Seção 5.6.

5.1 Contextualização do Assunto: Comunicação Anônima Segura em Grupo

Apresenta-se a seguir, novamente, a definição formal do problema:

Alice emite uma mensagem para Beto. Porém, Alice quer a garantia que, se Beto publicar a mensagem recebida de Alice, ele não tenha como provar que esta mensagem veio de Alice, mesmo Beto estando certo disso.

Para contextualização, particiona-se o problema acima formalizado, iniciando a análise pela última afirmação. Tem-se o seguinte:

"... mesmo Beto estando certo disto.- Essa afirmação diz respeito ao seguinte aspecto. Quais as maneiras que Beto teria para ter certeza de que a mensagem veio realmente de Alice?

A solução primeira e imediata seria usar um dos esquemas de identificação propostos no Capítulo 4. O esquema de identificação é suficiente para Alice se identificar frente a Beto. Porém, por si só, a identificação não é suficiente para garantir a integridade da mensagem passada para Beto, com a garantia que Beto necessita.

Para se alcançar a garantia de integridade e da autenticidade da mensagem pode-se incluir um resumo a um esquema de identificação genérico. Esta é uma solução viável e, fazendo assim, converte-se o esquema de identificação em um esquema de assinatura digital [SCH 96a]. Fazendo uso de um esquema de assinatura digital, a garantia de integridade e de autenticidade da mensagem estará garantida.

"... , ele não tenha como provar que esta mensagem veio de Alice, ...- Essa questão resume o principal desafio deste trabalho de pesquisa: oferecer uma solução a esta ambigüidade. Beto tem que ter certeza de que a mensagem veio de Alice, porém

não pode provar essa certeza a um terceiro. Assinando a mensagem digitalmente, Alice deixa sua identificação vinculada à mensagem, pois a assinatura de Alice para o documento em questão permanece e pode ser retransmitida por Beto.

5.2 A Solução Apresentada

A proposta de solução para o problema da comunicação anônima segura em grupo, apresentada nesse capítulo através da formalização de um protocolo criptográfico, assemelha-se bastante a alguns temas clássicos da criptografia, a seguir relacionados:

Assinatura Digital - A assinatura digital soluciona o problema da autenticação, aplicando as funcionalidades da assinatura tradicional em um documento digital.

A proposta de solução assemelha-se bastante a um processo de assinatura digital, porém não faz uso da Autoridade Confiável para divulgação da chave pública. Na solução apresentada, a chave assimétrica, que corresponderia à chave pública em um processo de assinatura digital convencional, é divulgada pelo próprio elemento receptor, Beto.

Chave de Sessão - A proposta de solução ao problema tem ainda fortes semelhanças a um processo de utilização de chaves de sessão, conforme apresentado na Seção 2.4, com algumas características especiais. Diferente do uso clássico das chaves de sessão, utiliza-se uma chave de sessão assimétrica e que deve ser gerada pelo receptor, Beto, incondicionalmente.

5.3 Protocolo Criptográfico: Comunicação Anônima Segura em Grupo

A formalização do protocolo proposto é baseada na Figura 5.1, onde apresentam-se os diversos elementos pertencentes ao protocolo que se propõe.

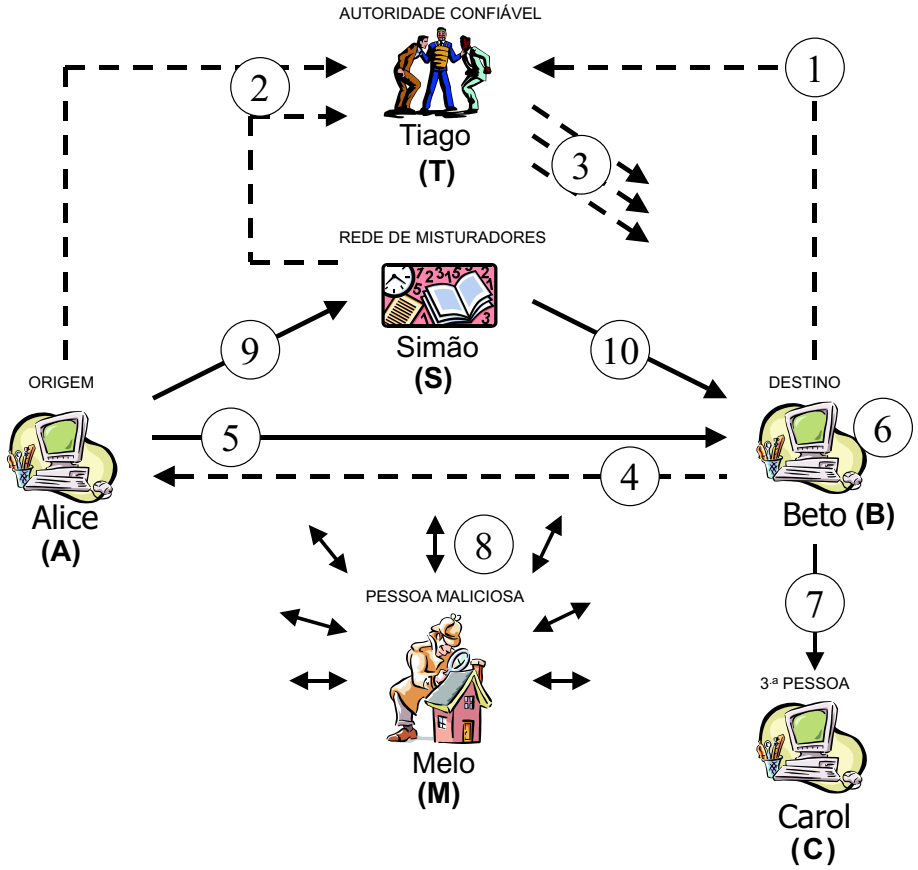

Figura 5.1: Protocolo Criptográfico Para Comunicação Anônima Segura em Grupo - Cada elemento que participa do esquema proposto está representado nesta figura. As linhas tracejadas representam a troca de chaves, e as linhas cheias representam a troca efetiva de informação. Os números entre círculo representam os passos a serem seguidos para descrição do protocolo.

Os elementos representados por computadores pessoais são os membros que participam do esquema, como usuários. Os outros dois elementos, Tiago e Simão, são os membros complementares, necessários no funcionamento do protocolo, compondo a Autoridade Confiável e a Rede de Misturadores, respectivamente. As setas representam o fluxo de informação, sendo que as linhas tracejadas são informações de repasse de chaves. As linhas cheias representam a informação propriamente dita, ou as mensagem confidenciais a serem trocadas. Os passos a serem seguidos estão representados pelos números entre parênteses. Detalha-se cada um desses passos a seguir:

Passo (1) - Beto gera um par de chaves assimétricas, KU_B e KR_B, e encaminha a chave

pública KU_B com a sua identificação ID_B para Tiago, por um canal seguro. Tiago será responsável pela divulgação da chave KU_B. A chave KR_B é mantida em segredo por Beto. Tiago tem a função de se certificar de que a chave informada por Beto realmente pertence a ele, pois cabe a ele, como sendo uma Autoridade Confiável responsável pela distribuição de chaves públicas. Uma maneira que Beto terá para entregar KU_B a Tiago, é cifrar KU_B e sua identificação ID_B com a chave pública de Tiago KU_T. Um resumo poderá ser gerado sobre esses dados para garantir a integridade da informação. Formalmente, tem-se o seguinte:

$$B \rightarrow T : E_{KU_T}(ID_B \| KU_B \| H(ID_B \| KU_B))$$

Passo (2) - Analogamente ao Passo (1), o mesmo procedimento é feito para divulgação da chave pública de Alice KU_A e de Simão KU_S. Formalmente, tem-se o seguinte:

$$A \rightarrow T : E_{KU_T}(ID_A \| KU_A \| H(ID_A \| KU_A))$$
$$S \rightarrow T : E_{KU_T}(ID_S \| KU_S \| H(ID_S \| KU_S))$$

Passo (3) - Tiago irá decifrar as informações recebidas e divulgará as chaves públicas KU_A, KU_B e KU_S para todos os elementos do esquema. Inclusive Melo terá acesso a essa informação.

Esta fase inicial serve para estabelecer uma forma prática de canais de comunicação confiáveis entre os elementos do sistema. O mesmo resultado pode ser obtido usando certificados digitais. Neste caso, Tiago seria uma Autoridade Certificadora. VeriSign, líder mundial de provisionamento de infra-estrutura segura na Internet, usa esta técnica. Dessa maneira, quando Beto quiser enviar uma informação de forma confiável para Alice, o mesmo poderá cifrar a mensagem com a chave KU_A, de maneira que somente Alice, que possui a chave KR_A, terá acesso à informação. A partir do Passo (4) começa o cerne do protocolo propriamente dito.

Passo (4) - Beto gera um novo par de chaves assimétricas K_1 e K_2, destinadas exclusivamente para a comunicação com Alice. A chave K_1, pública de Beto, será encaminhada a Alice por um canal seguro, juntamente com a identidade de Beto, ID_B. A chave $K2$, privada de Beto, será mantida em segurança por ele.

$$B \rightarrow A : E_{KU_A}(ID_B \| K_1 \| H(ID_B \| K_1))$$

Estas fases até o Passo (4) são as fases de inicialização, sendo executadas uma única vez, no momento que o sistema de comunicação for criado.

A partir do Passo (5) começa o processo de comunicação anônima segura propriamente dita.

As premissas que viabilizarão o protocolo a funcionar, conforme se deseja, são as seguintes:

- A chave pública de Beto, K_1, é a maneira que Alice tem para se identificar perante Beto. Desta maneira, Alice não teria interesse em divulgar K_1, pois uma terceira pessoa poderia enviar mensagens em seu nome para Beto.
- Beto não tem interesse em divulgar a chave pública, K_1, pois ao divulgá-la, Beto não teria mais como identificar quem efetivamente é o emissor da mensagem. Ou seja, Beto não teria como garantir que o emissor é mesmo Alice.

Mantendo-se as premissas acima descritas, a chave pública de Beto, K_1, irá representar uma informação de identidade de Alice que somente Beto conhece, permitindo que Alice se identifique perante Beto. Essa informação de identidade só tem validade para Beto.

Passo (5) - Alice quer enviar uma mensagem confidencial, M, para Beto. Alice cifrará a mensagem M com a chave pública de Beto, K_1, de maneira que somente Beto, que possui a chave privada K_2, poderá decifrar a mensagem. Um resumo poderá

ser inserido para garantia de integridade da informação. A descrição formal desse processo é a seguinte:

$$A \rightarrow B : E_{K_1}(M \| H(M)) \triangleright Y$$

Passo (6) - A mensagem confidencial cifrada, Y, é transmitida por Alice. Beto, ao receber a mensagem Y de Alice, decifra-a usando sua chave privada, K_2, recuperando a mensagem M. A única informação que identificará que a mensagem confidencial, Y, foi enviada por Alice será o fato da mesma ter sido cifrada com a chave pública de Beto, K_1. Somente Beto sabe que K_1 é de Alice K_1, pois foi gerada por Beto exclusivamente para comunicação com Alice. O processo executado por Beto está representado a seguir:

$$\text{Em } B\text{: } D_{K_2}(Y) \triangleright M \| H(M)$$

Prossegue-se o cálculo para verificação da integridade por Beto, recalculando o resumo da mensagem M recebida e comparando com o resumo recebido, $H(M)$. Dessa maneira, Beto certifica a integridade da mensagem recebida de Alice.

Passo (7) - Beto poderá resolver transmitir a mensagem M a Carol, e tem todo o direito de fazê-lo. Porém, Beto não terá como provar a Carol que esta mensagem foi originada por Alice. Beto poderá até dizer a Carol que foi Alice quem lhe enviara a mensagem M, mas não terá como provar esse fato.

Passo (8) - Melo representa uma pessoa maliciosa tentando burlar o esquema. Melo representa qualquer outro elemento, exceto Alice ou Beto, que usará de todos os artifícios para tentar descobrir a identidade do originador da mensagem M, Alice, em mensagens recebidas por Beto.

Monitorando os canais de comunicação, identificando o endereço de origem das mensagens, Melo poderá saber que Alice está se comunicando com Beto. Desta

maneira, para se aumentar ainda mais a garantia do anonimato de Alice, dificultando as ações de Melo, faz-se inserção do elemento chamado Simão, responsável por mascarar os dados de endereçamento, bem como, por eliminar qualquer relação estatística entre o tamanho das mensagens recebidas e encaminhadas. Isto constitui uma estrutura criptográfica chamada Rede de Misturadores [CHA 81]. A Rede de Misturadores habilita um grupo de usuários a trocar mensagens anônimas, eliminando qualquer relação entre os dados recebidos e enviados por cada um. Simão é um elemento de confiança, sem muita inteligência, cuja função fundamental é a de encaminhar as mensagens recebidas em fragmentos. Desta maneira, ao invés de Alice encaminhar a mensagem diretamente para Beto, ela encaminha para Simão que transfere a Beto, de maneira fragmentada. Simão não terá acesso à mensagem, pois estará cifrada com a chave pública de Beto, K_1.

Passo (9) - Alice enviará a Simão a mensagem M cifrada com a chave pública de Beto, K_1, juntamente com o endereço físico de Beto, N_B, por um canal seguro, cifrando-a com a chave pública de Simão, KU_S. O resumo poderá ser novamente usado, tanto na mensagem para Beto, quanto no endereço físico de Simão. Esse passo está sintetizado na representação formal abaixo:

$$A \rightarrow S : E_{KU_S}(N_B \| H(N_B) \| E_{K_1}(M \| H(M)))$$

Passo (10) - Simão decifrará a primeira parte da mensagem recebida de Alice com sua chave privada, KR_S, verificará a integridade do endereço físico recebido através do seu resumo, $H(N_B)$, e encaminhará a outra parte, $E_{K_1}(M \| H(M))$, para o endereço N_B. Simão receberá diversas mensagens de tamanho variável e encaminhará fragmentos de mensagem com tamanho fixo para o endereço N_B, dificultando qualquer associação entre o tamanho dos pacotes de entrada, emitidos por Alice, e o tamanho dos pacotes de saída, encaminhados para Beto. Mais uma vez, a única informação que certificará que a mensagem veio de Alice será o fato de Beto saber que sua chave pública, K_1, é de uso exclusivo de Alice. Nem mesmo Beto poderá associar

a mensagem recebida com o endereço de origem da mensagem recebida, pois todas as mensagens estarão vindo de Simão. Desta maneira, Beto sabe que a mensagem veio de Alice, mas não tem como provar isso a terceiros.

A Figura 5.2 ilustra os passos 9 e 10 do protocolo no processo de transmissão através da rede de misturadores.

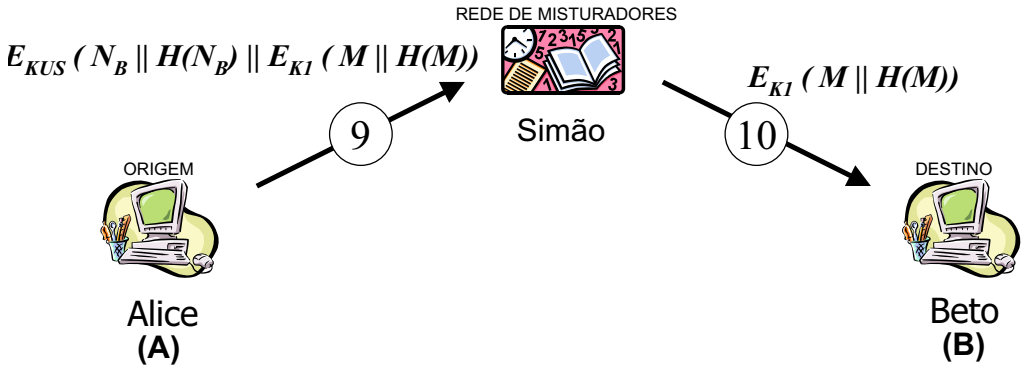

Figura 5.2: Uso da Rede de Misturadores no Protocolo Proposto - Alice, ao invés de transmitir a mensagem diretamente para Beto, transmite por intermédio de Simão, no Passo 9, por um canal seguro. Simão, por sua vez, retransmite a mensagem para Beto, em fragmentos da mensagem de tamanho fixo, no Passo 10.

5.3.1 Considerações Sobre a Segurança do Protocolo Proposto

Analisa-se aqui alguns aspectos de segurança do protocolo acima descrito. Beto gera um par de chaves para comunicação com Alice, e envia sua chave pública, K_1, para Alice que não deverá divulgá-la para ninguém. Será com essa chave que Alice se identificará perante Beto. Nesse sentido, as seguintes situações podem ser consideradas:

a) O que acontecerá se Alice divulgar a chave K_1?

Com Alice - Alice não terá mais como se autenticar perante Beto. É como se Alice tivesse passado uma procuração para um terceiro, que responderá por Alice frente a Beto.

Com Beto - Beto pensará que toda informação cifrada com a chave K_1 veio de Alice. Porém, nada impediria que Alice divulgasse a chave pública de Beto, K_1, e Beto não teria como saber quando isso teria ocorrido.

O interesse de Alice está no fato de que Beto vai acreditar que toda mensagem cifrada com sua chave pública associada a Alice, K_1, é proveniente da mesma, mesmo não tendo como provar isso a terceiros. Alice precisa desse tipo de comunicação com Beto. Nem mesmo Alice terá acesso à mensagem enviada por um terceiro que teve acesso à chave K_1, pois somente Beto possui a chave privada K_2 para decifrar a mensagem. Isso poderia desqualificar Alice em relação a Beto.

b) O que acontecerá se Beto entregar a chave K_1 de Alice para um terceiro?

Com Beto - Será de interesse de Beto que somente Alice possua a chave K_1, pois será a única maneira que Beto terá para saber que a mensagem M veio mesmo de Alice. Ao divulgar a chave K_1, Beto não iria saber exatamente quem encaminhou a mensagem. Como Beto não teria como provar a terceiros que a mensagem viera de Alice, o mesmo não teria motivos para tal.

c) O que acontecerá se Beto divulgar a chave K_2?

Com Beto - Se Beto divulgar a chave K_2, todas as pessoas que possuírem esta chave poderão ler a mensagem enviada por Alice. Porém, somente Beto saberá que a mensagem veio de Alice. Beto poderá até dizer que a mensagem veio de Alice, mas não teria como provar isso. Em condições normais, somente Beto terá acesso à informação e saberá que veio de Alice.

d) O que acontecerá se Beto enviar uma chave pública de Carol, K_1', para Alice, como sendo sua chave pública K_1?

Com Carol - Um terceiro elemento, por exemplo Carol, de comum acordo com Beto, poderia gerar um par de chaves K_1' e K_2' e enviar K_1' para Beto. Beto, tentando revelar a identidade de Alice para Carol, enviaria a chave K_1' como

sendo sua chave K_1. De qualquer maneira, Beto não teria como provar a Carol que a chave K_1' foi enviada somente a Alice. Como conseqüência, somente Carol, que possuiria a chave K_2', teria acesso à informação enviada por Alice. No entanto, Carol não teria como se certificar se a mensagem veio realmente de Alice, não teria a garantia que a chave K_1' tivesse sido efetivamente enviada a Alice por Beto. Beto pode ter divulgado K_1' para qualquer outro elemento.

Desta maneira, a proposta inicial se satisfaz, pois a identidade de Alice estará resguardada em qualquer situação. Ninguém, além de Beto, saberá a origem da informação.

O protocolo descrito é baseado no ”princípio do interesse mútuo”, e se isso acontecer, teremos uma forma interessante de comunicação.

Um terceiro, tal como Carol, pode vir a ter acesso à mensagem, mediante uma traição de Beto. Porém Beto não tem como provar que foi Alice quem lhe enviou a mensagem, deixando Carol na incerteza da origem da informação.

O anonimato de Alice está garantido de qualquer maneira, exceto para Beto, atendendo o propósito do protocolo.

Apresenta-se uma análise mais aprofundada sobre a segurança do protocolo proposto no Capítulo 6.

5.4 Funcionamento do Protocolo Proposto

No processo de inicialização, no Passo (4), Melo poderia tentar encaminhar uma mensagem divulgando uma chave K_1' como sendo a chave K_1 de Beto, tentando se passar por Beto. Desta maneira, Alice encaminharia mensagens para Melo pensando estar enviando para Beto. Um processo de assinatura digital poderia ser usado para que Alice tivesse certeza de que foi Beto quem lhe enviara a informação. Ao cifrar o resumo com sua chave KR_B, Beto provará para Alice ser ele quem está divulgando K_1. A mensagem toda, contendo a informação de K_1, deverá ser cifrada com a chave KU_A de Alice, de maneira que somente Alice poderá ter acesso à informação, como a seguir:

$$B \rightarrow A : E_{KU_A}(ID_B \| K_1 \| E_{KR_B}(H(ID_B \| K_1)))$$

Desta maneira, Alice se certificará que Beto é, efetivamente, o emissor da informação recebida. Como conseqüência, Alice terá como provar que Beto também tem conhecimento da chave K_1. Com isso, Alice poderá comprovar que Beto conhece a mensagem por ela enviada. Não é de interesse de Alice fazê-lo, pois estaria confessando ser ela mesma a fonte da informação. É de interesse de Alice manter seu anonimato na mensagem enviada a Beto. Esse passo é de fundamental importância no funcionamento do protocolo.

Ainda no Passo (4), onde Beto gera o par de chaves assimétricas K_1 e K_2, poderia ser usada uma chave simétrica K única, a ser divulgada para Alice. Os princípios do protocolo se mantém, a menos do seguinte problema. Alice, de posse da chave K poderia querer divulgá-la para um terceiro. Fazendo-o, Alice passaria a ter acesso às mensagens encaminhadas por este terceiro a Beto, o que daria a Alice uma maior segurança para divulgar a chave K. Isto poderia vir a desqualificar o protocolo. Usando-se chaves assimétricas, se Alice divulgar a chave K_1 recebida de Beto, nem mesmo Alice poderia ter acesso às informações enviadas a Beto em seu nome, o que proporcionaria uma maior segurança ao protocolo.

Considerações ainda se fazem necessária em relação ao Passo (5). A maneira como a mensagem foi encaminhada no Passo (5) representa perfeitamente o funcionamento do protocolo, de maneira didática. Porém, na prática, não se usam chaves assimétricas, no caso K_1 e K_2, para cifrar mensagens. O uso mais comum das chaves assimétricas é para distribuição das chaves simétricas. As chaves simétricas irão posteriormente ser efetivamente usada para cifrar e decifrar as mensagens, conforme apresentado na Seção 2.4.

Formalmente tem-se o seguinte:

$$A \rightarrow B : E_{K_1}(K \| H(K)) \| E_K(M \| H(M)) \triangleright Y$$

A Figura 5.3 ilustra este processo. As mudanças não alteram o funcionamento básico do protocolo, uma vez que a chave K é de uso transitório, podendo até ser uma chave de sessão.

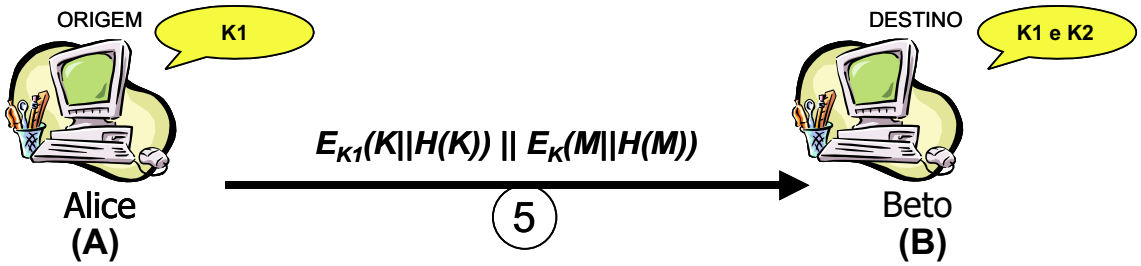

Figura 5.3: Passo 5 com Chave Simétrica - Ao invés de cifrar a mensagem $M||H(M)$ com a chave assimétrica $K1$, Alice cifra uma chave simétrica $K||H(K)$ com K_1, em seguida cifra a mensagem $M||H(M)$ com a chave K e tramite ambas.

5.5 Extensão do Protocolo Para Comunicação Anônima Segura em Grupo

Nesta seção, estende-se o comportamento do protocolo proposto para a comunicação anônima segura entre um grupo de usuários, e não mais somente entre Alice de Beto. O objetivo é analisar o processo de distribuição das chaves assimétricas, K_1 e k_2, quando se necessita de uma comunicação entre vários os elementos, e não somente Alice emitindo mensagens para Beto. Verifica-se assim as implicações na geração, manuseio e utilização das chaves assimétricas.

Para se fazer a análise acima descrita, divide-se esta seção nas seguintes subseções.

Na Subseção 5.5.1 faz-se uma descrição da notação a ser usada para identificação das chaves assimétricas, K_1 e K_2, a serem distribuídas entre os elementos que participarão do processo de comunicação anônima segura em grupo. Na Subseção 5.5.2 analisa-se a necessidade de geração, e armazenamento das chaves assimétricas, K_1 e K_2, por cada elemento do grupo. Na Subseção 5.5.3 faz-se as considerações da extensão

do protocolo para uso em uma comunicação anônima segura entre um grupo de usuários.

5.5.1 Notação Específica Para Comunicação em Grupo

Para facilitar a explanação, considera-se um grupo de quatro elementos. Um dos elementos é Alice, que irá se comunicar de forma anônima e segura com os outros três elementos. Os quatro elementos são os seguintes:

Alice (A) - Emissor da Mensagem.
Beto (B) - Receptor 1 da mensagem M.
Carol (C) - Receptor 2 da mensagem M.
Davi (D) - Receptor 3 da mensagem M.

As chaves K_1 e K_2 serão agora chamadas K_{ij1} e K_{ij2}, onde i representa o elemento receptor da mensagem M, que gera o par de chaves assimétricas, e j representa o elemento emissor da mensagem M, para quem a chave K_{ij1} será encaminhada.

O exemplo a seguir ilustra o uso das chaves K_{ij1} e K_{ij2}. Beto, destino $i = B$, gera um par de chaves assimétricas para comunicação anônima segura com Alice, origem $j = A$. As até então chaves K_1 e K_2, agora ficam K_{BA1} e K_{BA2}, respectivamente. Ou seja, a chave K_1 gerada por Beto para Alice fica K_{BA1}, e a chave K_2 a ser enviada para Alice por Beto fica K_{BA2}.

5.5.2 Distribuição das Chaves Para Comunicação Anônima Segura em Grupo

Todos os elementos devem gerar pares de chaves para comunicação anônima segura entre si. As chaves públicas de i, K_{ij1}, devem ser enviadas de i para j, e as chaves privadas de i, K_{ij2}, ficam secretamente armazenadas por i. A Figura 5.4 ilustra a distribuição das chaves no grupo, supondo que todas as chaves K_{ij1} e K_{ij2} foram geradas, e todas as chaves K_{ij1} foram enviadas para o destino j específico.

Pode-se, então, tirar as seguintes conclusões:

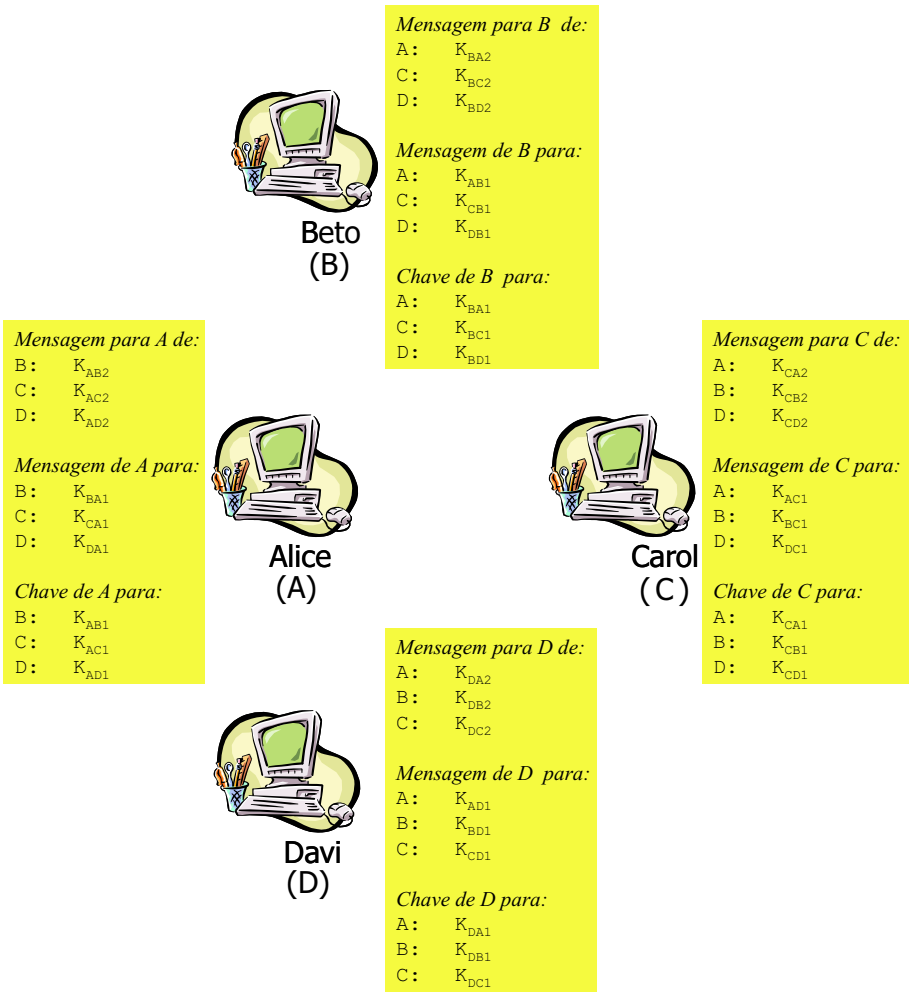

Figura 5.4: Distribuição das Chaves no Grupo - Representa-se as chaves necessárias para comunicação de quatro elementos entre si.

- Alice, por exemplo, tem que gerar três pares de chaves:

  - K_{AB1} - Chave que Alice enviará a Beto que irá usá-la para enviar mensagens confidenciais a Alice.

  - K_{AC1} - Chave que Alice enviará a Carol que irá usá-la para enviar mensagens confidenciais a Alice.

  - K_{AD1} - Chave que Alice enviará a Davi que irá usá-la para enviar mensagens confidenciais a Alice.

  - K_{AB2} - Chave que Alice irá usar para decifrar as mensagens confidenciais rece-

bidas de Beto.

- K_{AC2} - Chave que Alice irá usar para decifrar as mensagens confidenciais recebidas de Carol.
- K_{AD2} - Chave que Alice irá usar para decifrar as mensagens confidenciais recebidas de Davi.

- Alice recebe ainda mais três chaves:
  - K_{BA1} - Chave que Beto enviará a Alice que irá usar para enviar mensagens confidenciais a Beto.
  - K_{CA1} - Chave que Carol enviará a Alice que irá usar para enviar mensagens confidenciais a Carol.
  - K_{DA1} - Chave que Davi enviará a Alice que irá usar para enviar mensagens confidenciais a Davi.

- Analogamente, a mesma quantidade de chaves será manuseada pelos outros elementos: Beto, Carol e Davi.

- Desta maneira, pode-se concluir que a quantidade de chaves, nK, a serem geradas por um elemento é diretamente proporcional à quantidade de elementos do grupo, conforme demonstrado a seguir:

$$nG\text{: } nK = 2 \times (nG - 1)$$

  No exemplo, para um grupo de quatro elementos, tem-se o seguinte:

$$nK = 2 \times (4 - 1) = 6$$

- Das nK chaves geradas por cada elemento, $nK/2 = (nG - 1)$ chaves devem ser distribuídas para os outros elementos.

- Após a distribuição das $nK/2$ chaves, cada elemento estará manuseando nK chaves, sendo $nK/2$ chaves privadas geradas localmente, e $nK/2$ chaves públicas recebidas dos outros elementos.

5.5.3 Considerações Sobre o Uso do Protocolo Para Comunicação Anônima Segura em Grupo

Quando se estende o conceito do protocolo proposto para um grupo de usuários que se comunicam em ambos os sentidos, de forma anônima e segura, a quantidade de chaves pode tomar grandes proporções e, uma análise específica se faz necessária. A identificação da origem das mensagens recebidas é única e exclusivamente dependente da chave K_{ij1}. Com uma quantidade considerável de elementos no grupo, a identificação das mensagens se torna crítica, uma vez que cada uma das chaves deve ser testada para identificação da origem. A busca de uma maneira eficaz de identificar o emissor das mensagens, ou uma nova proposta que venha a minimizar este problema, ficam como uma sugestão para trabalhos futuros.

A limitação acima descrita deixa de ser significativa, quando o protocolo é destinado a uma aplicação onde existe apenas um elemento receptor, como por exemplo: pagamento eletrônico via Internet, sistema de votação digital e sistema de leilão público via Internet, tal como apresentados na Seção 1.3.

Outra característica interessante do protocolo é a possibilidade de se fazer uma difusão de uma mensagem para todos os elementos do grupo, sem sigilo, porém, somente um dos elementos que conhece a chave K_{ij1} saberá a origem específica da mensagem. Para isto, basta alterar a maneira de cifrar a mensagem no Passo 5, conforme demonstrado a seguir:

Antes:	$A \rightarrow B : E_{K_{ij1}}(M \| H(M)) \triangleright Y$
Sugestão:	$A \rightarrow B : E_{K_{ij1}}(H(M)) \| M \triangleright Y$

Desta maneira, todos elementos terão acesso à mensagem, porém, so-

mente Beto saberá que foi Alice quem enviou esta mensagem. Obviamente, continua valendo que nem mesmo Beto poderá comprovar a um terceiro a origem da mensagem.

Outra característica interessante deste protocolo é que o subgrupo de pessoas com quem Alice pode se comunicar pode ser independente do grupo de pessoas que Beto se comunica, bem como de Carol e Davi. Desta maneira, os elementos têm conhecimento apenas do seu subgrupo, sendo que ninguém precisa ter conhecimento do grupo como um todo. Essa característica se faz presente devido a independência na geração das chaves simétricas, K_{ij1} e K_{ij2}. Supõe-se que Beto é um elemento receptor i que gera o par de chaves assimétricas, K_{ij1} e K_{ij2}, e encaminha K_{ij1} para os elementos emissores, j, de seu subgrupo. Beto não tem controle sobre quais pares de chaves assimétricas, K_{ij1} e K_{ij2}, estão sendo pelos outros elementos de seu subgrupo e, conseqüentemente, ele não conhece o grupo como um todo.

As seguintes alternativas para a comunicação entre Alice e Beto, por exemplo, ainda são possíveis:

- *Mensagem Restrita* - Alice poderá enviar a mensagem M cifrada com K_{BA1}, de maneira que somente Beto terá acesso à informação. Este é o tipo de mensagem usualmente considerado no protocolo proposto.

- *Mensagem Identificada* - Alice poderá divulgar uma mensagem anônima, cujo conteúdo poderá ser de conhecimento de todos, por um processo de difusão tal como apresentado na Seção 4.6. Se Alice assinar a mensagem com K_{BA1}, todos terão acesso à informação, mas somente Beto saberá que a mensagem veio de Alice.

- *Mensagem Aprazada* - Se Alice cifrar a mensagem com uma chave K genérica, sendo K uma chave simétrica de conhecimento único de Alice, e transmitir a mensagem para Beto assinada com K_{BA1}, consegue-se uma característica interessante. Beto receberá a mensagem, saberá que veio de Alice, porém somente poderá conhecer seu conteúdo após Alice divulgar a chave K para Beto.

5.6 Conclusão

Apresentou-se, neste capítulo, a formalização de um protocolo criptográfico capaz de tornar viável uma comunicação anônima segura em grupo, sendo esse o objetivo maior deste trabalho.

Fez-se uma analogia da proposta apresentada com temas clássicos da literatura sobre criptografia, buscando facilitar o entendimento do protocolo proposto.

O protocolo foi descrito passo a passo, previamente considerando-se uma comunicação entre dois elementos. Após sedimentados os conceitos fundamentais, fez-se a extensão para comunicação entre um grupo de elementos.

Como resultado, obteve-se um protocolo de fácil implementação, uma vez que é fundamentado em temas clássicos e bastante difundidos da criptografia, representando uma alternativa imediata para tornar viável uma comunicação anônima segura em grupo.

Algumas alternativas de uso do protocolo ainda foram sugeridas, ampliando as possibilidades de aplicação do mesmo.

Fez-se ainda, a identificação de pontos a serem melhorados. Um desses pontos é que o número de chaves criptográficas é proporcional ao tamanho do grupo e, para esse caso, apresentou-se as aplicações mais apropriadas para o uso do protocolo. Fez-se ainda as sugestões de melhorias a serem implementadas em trabalhos futuros.

Em resumo, o propósito principal do protocolo foi alcançado, que é a busca de uma alternativa que torne viável uma comunicação anônima segura em grupo.

Capítulo 6

Análise de Segurança

Uma análise da segurança oferecida pelo protocolo proposto no Capítulo 5 se faz necessária, no intento de comprovar a efetividade do mesmo. O objetivo é analisar seu comportamento mediante os diversos tipo de ataques possíveis.

Para tanto, apresenta-se os principais tipos de ataques na Seção 6.1. Posteriormente, na Seção 6.2, faz-se a análise do comportamento do protocolo mediante os diversos tipos de ataques possíveis, previamente apresentados.

6.1 Tipos de Ataques em Uma Rede de Comunicação de Dados

Considerando que a função fundamental de um sistema de comunicação de dados é prover troca de informação, em geral, existe um fluxo de informação entre uma origem genérica A para um destino B. O fluxo normal da informação, sem restrição de espécie alguma, está representado na Figura 6.1.

A caracterização de um ataque a um sistema de computação, ou a uma rede de computadores, pode se dar de várias maneiras. Os tipos de ataque podem ser divididos em quatro categorias genéricas:

Interrupção - Este ataque consiste em tornar o acesso à informação indisponível. Este é um ataque à **disponibilidade** da informação e está ilustrado na Figura 6.2. Uma

Figura 6.1: Caracterização do Fluxo normal da informação - Esta é a representação do fluxo normal da informação entre dois pontos, A e B.

interrupção do processo de comunicação é um ataque onde a informação transmitida por A não chega até B.

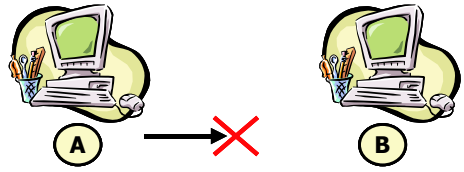

Figura 6.2: Caracterização do Ataque de Interrupção - Esta é a representação de um ataque de interrupção do processo de comunicação, onde a informação transmitida por A não chega até B.

Interceptação - Um elemento não autorizado ganha acesso a uma informação restrita. Este é um ataque à **confidencialidade** da informação e está ilustrado na Figura 6.3. Neste tipo de ataque, a informação transmitida de A para B, embora alcance B, é interceptada por um elemento C não autorizado, no meio do caminho.

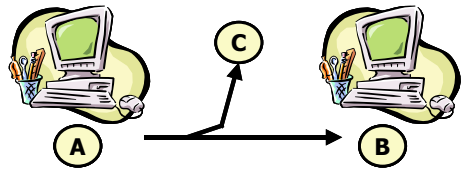

Figura 6.3: Caracterização do Ataque de Interceptação - Este é um ataque de interceptação da informação, onde a informação transmitida de A para B, embora alcance B, é interceptada por um elemento C não autorizado, no meio do caminho.

Modificação - Um elemento não autorizado, além de ganhar acesso a uma informação restrita, altera-a. Este é um ataque à **integridade** da informação e está ilustrado na

Figura 6.4. A informação transmitida de A para B é interceptada, com a interrupção da comunicação, e é indevidamente alterada por C. Depois C encaminha a mensagem alterada a B, personificando o emissor A.

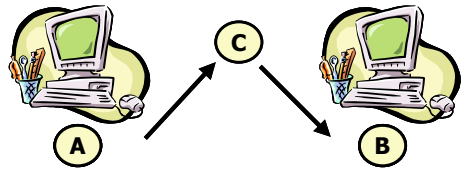

Figura 6.4: Caracterização do Ataque de Modificação - Um ataque de modificação da informação é representado nessa figura. A informação transmitida de A para B é indevidamente alterada por C.

Fabricação - Este ataque consiste em um elemento não autorizado inserir informações no sistema. Este é um ataque à **autenticidade** da informação e está ilustrado na Figura 6.5. Nessa situação, C envia uma informação para B personificando o emissor A.

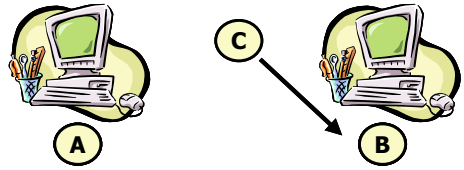

Figura 6.5: Caracterização do Ataque de Fabricação - Esta é a representação de um ataque de fabricação da informação. Nessa situação, C envia uma informação para B personificando o emissor A.

Na análise específica do protocolo proposto, as duas formas de ataques ao processo de identificação de Alice frente a Beto, a saber passivos e ativos, devem ser levados em consideração. Esses ataques estão descritos na Seção 4.1.

Tal como em um esquema de identificação, nosso protocolo será dito quebrado se um adversário não autorizado personificar Alice, fazendo com que Beto aceite a prova indevidamente, ou ainda, se Alice se identificar frente a um terceiro elemento malicioso, pensando estar se identificando frente a Beto.

Baseando-se nas definições acima, faz-se uma análise sobre os aspectos de segurança do protocolo, partindo do princípio de que as premissas estabelecidas na Seção 5.3, necessárias para viabilizar o protocolo, estão satisfeitas.

6.2 Segurança do Protocolo Proposto

Faz-se aqui uma análise do protocolo proposto, prevendo as possibilidades de ataques à disponibilidade, confidencialidade, integridade e autenticidade da mensagem enviada de Alice a Beto, nas Subseções 6.2.1, 6.2.2, 6.2.3 e 6.2.4, respectivamente. Verifica-se ainda, na Subseção 6.2.5, a questão relativa ao anonimato de Alice frente a terceiros. Finalmente, na Subseção 6.2.6, faz-se as considerações sobre a possibilidade de Alice querer, posteriormente, negar uma mensagem enviada a Beto.

6.2.1 Ataques à Disponibilidade

Alice envia uma mensagem para Beto, porém a mensagem não chega até seu destino. Os motivos que podem interromper o fluxo de informações entre Alice e Beto são bastante amplos: conexões físicas, *hardware* adulterado ou com problema, configuração dos equipamentos de roteamento adulterado ou inadequado, entre outros.

O protocolo que aqui propomos trabalha no nível de aplicação, destinado ao envio e recebimento de mensagens anônimas seguras entre um grupo de usuários de um sistema aberto de comunicação de dados. Este tipo de ataque, ou até mesmo em situações de falha, é tratado pelos níveis inferiores. Para o contexto dessa pesquisa, esse tipo de ataque não é considerado.

6.2.2 Ataques à Confidencialidade

Um elemento não autorizado, por exemplo Melo, poderá estar monitorando os canais de comunicação. Desta maneira, este elemento poderá estar buscando algumas das informações a seguir descritas:

- *Melo busca ter acesso à informação passada de Alice para Beto* - Considerando-se que todo o processo de inicialização ocorreu dentro da normalidade, as mensagens enviadas de Alice a Beto estarão cifradas pela chave K_1, e a única pessoa que conhece o par de chaves correspondente, K_2, é Beto. Não conhecendo a chave K_2, Melo terá extrema dificuldade para recuperar a mensagem original, uma vez que este é tido como um problema de difícil solução computacional, conforme visto na Seção 2.3.

- *Melo busca identificar que a comunicação está sendo feita entre Alice e Beto* - Monitorando os canais de comunicação, Melo poderá tentar descobrir que Alice está se comunicando com Beto, mesmo sem ter acesso à informação trocada entre eles. O uso da Rede de Misturadores objetiva dificultar as ações de Melo nesse sentido. A Seção 2.8 apresenta o uso das Redes de Misturadores, cuja função específica é garantir o anonimato de Alice.

- *Melo busca levantar informações sobre o processo de identificação de Alice frente a Beto* - O interesse de Melo por esses dados é para futuramente se identificar frente a Beto como sendo Alice, ou receber as mensagens de Alice como sendo Beto. A única maneira que Melo tem para personificar Alice, ou para decifrar a mensagem enviada para Beto, passando-se por Beto, é tendo acesso a alguma das chaves K_1 ou K_2. Em se mantendo as premissas do protocolo, as chaves K_1 e K_2 são restritas a Alice e a Beto, sendo K_2 de conhecimento único de Beto. A maneira que Melo teria para ter acesso à chave K_1 seria no Passo (4) do processo de inicialização, porém, a chave gerada por Beto é enviada por um caminho seguro até Alice. Se nem Beto nem Alice divulgarem as chaves, Melo não poderá se identificar frente a Beto e nem se passar por Beto.

Existe uma alternativa de uso do protocolo, onde a confidencialidade da mensagem M não é necessária, ou seja, em aplicações nas quais o conteúdo da mensagem é de livre acesso, mantendo-se apenas a questão do anonimato de Alice. O resumo da mensagem, $H(M)$, é cifrado com K_1 por Alice, de maneira que somente Beto, que possui a chave K_2, saberá a origem específica da mensagem.

6.2.3 Ataques à Integridade

A integridade da mensagem passada de Alice para Beto é garantida pelo resumo que está agregado à mensagem, $H(M)$, conforme definições da Seção 2.5. Qualquer alteração na mensagem originalmente enviada por Alice poderá ser identificada por Beto no destino. Nesse caso, Beto irá desconsiderar a mensagem recebida.

6.2.4 Ataques à Autenticidade

A autenticidade da informação enviada de Alice a Beto está diretamente relacionada à chave K_1. Melo, não conhecendo a chave K_1, não terá como forjar uma mensagem enviada para Beto, como sendo de Alice. Qualquer mensagem que não seja cifrada com a chave K_1 será facilmente verificada por Beto como não sendo uma mensagem válida, tendo Alice como emissor.

6.2.5 Ataques ao Anonimato do Emissor

Monitorando os canais de comunicação, um elemento malicioso, Melo, poderá tentar quebrar o anonimato de Alice, em mensagens enviadas a Beto pelo sistema de comunicação anônima segura em grupo. A única maneira que Beto tem para identificar a mensagem M como sendo de Alice é pelo fato da mensagem M estar cifrada com a chave pública de Beto, K_1. Da mesma maneira, Melo, para identificar o emissor deverá saber que K_1 pertence a Alice. Em se mantendo as premissas do protocolo, o único elemento que sabe que K_1 pertence à Alice é Beto. Beto pode até dizer para Melo que K_1 pertence à Alice, mas não tem como provar esse fato. Desta maneira, o anonimato de Alice perante um terceiro qualquer está garantido, sob qualquer circunstância.

6.2.6 Considerações Sobre o Não-Repúdio do Emissor

Supõe-se que, por algum motivo específico, Alice se arrependa de ter enviado uma mensagem M para Beto. A mensagem enviada por Alice estará cifrada com a chave pública de Beto, K_1, que, mantendo-se as premissas do protocolo, é de

conhecimento exclusivo de Alice e Beto. Dessa maneira, Alice não terá como negar uma mensagem enviada a Beto, pois, além do próprio Beto, Alice é a única que conhece K_1.

6.3 Conclusão

Apresentou-se, neste capítulo, as diversas possibilidades de ataques a um sistema aberto de comunicação de dados, conforme identificado na literatura.

Analisou-se, então, os aspectos de segurança do protocolo proposto mediante as possibilidades de ataques levantadas, atestando a efetividade e aplicabilidade do mesmo.

A segurança de um protocolo criptográfico, em muitas situações, está diretamente relacionada com as técnicas envolvidas e, neste caso específico, por se tratarem de técnicas bastante difundidas da criptografia, obtém-se um índice elevado de segurança, desde que respeitadas as premissas de funcionamento do mesmo.

Capítulo 7

Considerações Finais

Faz-se as considerações finais desse trabalho de pesquisa em duas seções:

- Na Seção 7.1, apresenta-se as conclusões do resultado obtido com esse trabalho de pesquisa.

- Na Seção 7.2, faz-se algumas sugestões de trabalhos futuros.

7.1 Conclusões

Apresentou-se, nesse trabalho de pesquisas, um breve estudo sobre os principais fundamentos da criptografia, com ênfase aos assuntos que mais se identificam com o tema principal: Comunicação Anônima Segura em Grupo.

Com base em um sólido embasamento teórico, fez-se a apresentação de uma proposta de implementação, que torne viável uma comunicação entre um grupo de usuários de um sistema aberto de comunicação de dados, de forma anônima segura.

O objetivo principal, deste trabalho de pesquisa, que é apresentar uma alternativa para uma comunicação anônima segura em grupo, foi alcançado. Uma solução para o problema foi apresentada, descrita e discutida, assim como suas limitações e melhorias necessárias.

Por se tratar do uso de técnicas difundidas e consagradas da criptografia, a solução aqui apresentada é de fácil implementação, confirmando-se como uma alterna-

tiva de solução prática e imediata para o problema proposto.

O protocolo formalizado tem sido amplamente usado no LabSEC, Laboratório de Segurança em Computação da UFSC. Esse protocolo foi implementado como parte de um processo de leilão público via Internet, desenvolvido pelo LabSEC. A alternativa de comunicação anônima segura em grupo, tal como proposto nesse trabalho, representa uma sensível evolução nos processos criptográficos desenvolvidos no LabSEC, uma vez que esta alternativa de comunicação não foi encontrada de maneira clara na literatura, até então.

O protocolo proposto apresenta uma enorme flexibilidade, sendo possíveis as seguintes alternativas de implementação:

- Transmissão anônima segura com ou sem confidencialidade.
- Transmissão anônima segura direta ou para um grupo de pessoas, de maneira que somente um elemento irá identificar o emissor.
- Transmissão anônima segura com posterior identificação do emissor.
- Transmissão anônima segura com identificação imediata do emissor e posterior revelação do conteúdo.

Com isso, pode-se ampliar a aplicabilidade do mesmo, aumentando ainda mais as alternativas de uso, sendo algumas dessas alternativas sugeridas na Seção 1.3.

7.2 Trabalhos Futuros

Como sugestões de trabalhos futuros, objetivando implementar melhorias na proposta apresentada neste trabalho de pesquisa, pode-se relacionar o seguinte:

- Implementação deste protocolo em computadores pessoais em larga escala, visando avaliar o comportamento em função do volume de mensagens, verificando a necessidade de usar servidores específicos, analisando o impacto no manuseio de um

número elevado de chaves criptográficas e, mensurando a necessidade de processamento para identificação das mensagens no destino.

- Apresentação de um processo eficiente para Beto verificar as mensagens recebidas, dada a enorme quantidade de chaves K_{ij2} que Beto tem para identificar a origem específica da mensagem, uma vez que, no processo original as mensagens devem ser testadas com cada uma das chaves, pois a chave é a única forma de identificação de Alice frente a Beto.

- Apresentação de melhorias que possam diminuir a necessidade de um número elevado de chaves K_{ij1} e K_{ij2}, proporcional ao tamanho do grupo, de maneira que a quantidade de chaves seja independente do tamanho do grupo.

- Identificar ou desenvolver um processo de modelagem formal, capaz de provar a segurança oferecida por um protocolo criptográfico, bem como, comprovar a dificuldade computacional de quebra do anonimato.

Referências Bibliográficas

[ADA 93] ADAMS, C. M.; TAVARES, S. E. Designing s-boxes for ciphers resistant to differential cryptanalysis. **Proceedings of the 3rd Symposium on State and Progress of Research in Criptography**, [S.l.], p.181–190, 1993.

[BLA 79] BLAKLEY, G. R. Safeguarding cryptographic key. **AFIPS**, [S.l.], p.313–317, 1979.

[BUR 90] BURROWS, M.; ABADI, M.; NEEDHAM, R. A logic of authentication. **ACM**, [S.l.], p.18–36, 1990.

[CAR 97] CARDOSO, J. **Redes de Petri**. UFSC, 1997.

[CHA 81] CHAUM, D. Untraceable electronic mail, return addresses, and digital pseudonyms. **EUROCRYPT'91**, [S.l.], 1981.

[CHA 83] CHAUM, D. Blind signatures for untraceable payments. **CRYPTO'82**, [S.l.], 1983.

[CHA 91] CHAUM, D.; HEYST, E. V. Group signatures. **EUROCRYPT'91**, [S.l.], 1991.

[CHE 94] CHEN, L.; PEDERSEN, T. P. New group signature schemes. **Advance in Cryptology: proceedings of Eurocrypt'94**, [S.l.], p.171 – 181, 1994.

[DES 85] Ansi x9.17. **American National Standard for Financial Institution Message Authetication (Wholesale)**, [S.l.], 1985.

[DIF 76] DIFFIE, W.; HELLMAN, M. New directions in cryptography. **IEEE Transations on Informations Theory**, [S.l.], v.22, n.6, p.644–654, 1976.

[DOL 83] DOLEV, D.; YAO, A. On the security of public-key protocols. **IEEE**, [S.l.], p.198–203, 1983.

[FAN 00] FAN, C.-I.; CHEN, W.-K.; YEH, Y.-S. Randomization enhaced chaum's blind signature scheme. **Computer Communications**, [S.l.], v.23, p.1677–1680, 2000.

[FEI 87] FEIGE, U.; FIAT, A.; SHAMIR, A. Zero-knowledge proofs of identity. **Proceedings of 19th ACM Symposium of Theory of computing**, [S.l.], p.210–217, 1987.

[FEI 88] FEIGE, U.; FIAT, A.; SHAMIR, A. Zero-knowledge proofs of identity. **Journal of Criptology, v.1 n. 2**, [S.l.], p.77–94, 1988.

[FIA 86] FIAT, A.; SHAMIR, A. How to prove yourself: practical solutions of identification and signature problems. **Crypto'86**, [S.l.], p.186–194, 1986.

[FIA 98] FIAT, A.; NAOR, M. Broadcast encryption. **CRYPTO'93**, [S.l.], p.480–491, 1998.

[GOL 85] GOLDWASSER, S.; MICALI, S.; RACKOFF, C. The knowledge comlexity of interactive proofs systems. **Proceedings of 17th ACM Symposium of Theory of computing**, [S.l.], p.291–304, 1985.

[GRI 99] GRITZALIS, S. Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification. **Computer Communications**, [S.l.], p.697–709, 1999.

[ING 90] INGEMARSSON, I.; SIMMONS, G. J. A protocol to set up shared secret schemes winthout assistance of a mutually trusted party. [S.l.], 1990.

[KEM 94] KEMMERER, R.; MEADOW, C.; MILLEN, J. Three systems for criptographic protocol analysis. **Journal of Criptology**, [S.l.], p.79–130, 1994.

[KIM 02] KIM, M.; KIM, K. **A New Identification Scheme based on the Bilinear Diffie-Hellman Problem**.

[KOH 78] KOHNFELDER, L. **Towards a Practical Public-Key Cryptosystem**. M.I.T., May, 1978. Tese de Doutorado.

[LAI 90] LAI, X.; MASSEY, J. A proposal for a new block encryption standard. **EUROCRYPT'90**, [S.l.], p.389–404, 1990.

[LAI 91] LAIH, C. S.; CHEN, C. H. Threshold identification. **IEEE**, [S.l.], p.73–76, 1991.

[LEE 97] LEE, G.-S.; LEE, J.-S. Petri net based models for specification and analysis of cryptographic protocols. **Elsevier Science Inc.**, [S.l.], p.141–159, 1997.

[LON 92] LONGLEY, D.; RIGBY, S. An automatic search for security flaws in key management schemes. **Computer and Security**, [S.l.], p.75–89, 1992.

[MAZ 90] MAZIERO, C. A. **ARP - Analisador de Redes de Petri - Disponível em *www.ppgia.pucpr.br/maziero***.

[MIC 88] MICALI, S.; SHAMIR, A. An improvement of the fiat-shamir identification and signature scheme. **CRYPTO'88**, [S.l.], p.244–247, 1988.

[OKA 92] OKAMOTO, T. Provably secure and practical identification schemes and corresponding signature schemes. **Crypto'92**, [S.l.], p.31–53, 1992.

[PAR 97] PARK, S.; KIM, S.; WON, D. Id-based group signature. **Eletronic Letter 33**, [S.l.], p.1616–1617, 1997.

[PET 81] PETERSON, J. Petri nets theory and the modeling of systems. **Prentice-Hall**, [S.l.], 1981.

[RIV 78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. **Communications of the ACM**, [S.l.], v.21, n.2, p.120–126, 1978.

[RIV 95] RIVEST, R. L. The rc5 encryption algorithm. **Dr. Dobb's Journal**, [S.l.], p.146–148, 1995.

[RIV 97] RIVEST, R. A description of the rc2(r) encryption algorithm. **Internet Draft**, [S.l.], 1997.

[SCH 89] SCHNORR, C. P. Efficient identification and signatures for smart cards. **CRYPTO'89**, [S.l.], p.239–252, 1989.

[SCH 94] SCHNEIER, B. Description of a new variable-lenght key, 64-bit block cipher (blowfish). **Fast Software Encryption, Cambridge Security Workshop Proceedings**, [S.l.], p.191–204, 1994.

[SCH 96a] SCHNEIER, B. **Apllied Cryptography**. United States of America: John Wiley Sons, Inc., 1996.

[SCH 96b] SCHNORR, C. P. Security of 2^t-root identification and signatures. **Crypto'96**, [S.l.], p.143–156, 1996.

[SHA 79] SHAMIR, A. How to share a secret. **ACM**, [S.l.], p.612–613, 1979.

[SHA 84] SHAMIR, A. Identity-based cryptosystems and signature schemes. **Crypto'84**, [S.l.], p.47–53, 1984.

[SHO 96] SHOUP, V. On the security of a practical identification scheme. **Crypto'96**, [S.l.], p.340–353, 1996.

[SNE 92] SNEKKENES, E. Roles in criptographic protocols. **IEEE**, [S.l.], p.105–119, 1992.

[STA 99] STALLINGS, W. **Cryptography and Network Security**. 2. ed. Upper Saddle River, NJ: Prentice-Hall, 1999. 569 p.

[TSE 98] TSENG, Y.-M.; JAN, J.-K. A novel id-based group signature. **Information Science**, [S.l.], v.120, p.131–141, jul, 1998.

[VAR 90] VARADHRAJAN, V. Petri net based modeling of information flow security requeriments. **Proc. the Computer Security Foundations Workshop**, [S.l.], p.51–61, 1990.

[WOO 91] WOO, T.; LAM, S. A semantic model for authentication protocols. **IEEE**, [S.l.], p.178–194, 1991.

Apêndice A

Modelagem do Protocolo Proposto em Redes de Petri

Faz-se aqui a modelagem do Protocolo Proposto em Redes de Petri, com objetivo de avaliar o funcionamento do protocolo criptográfico proposto neste trabalho de pesquisa.

Com objetivo de focar as funcionalidades específicas do protocolo proposto, consideram-se as seguintes condições iniciais: cada elemento participante do protocolo, Alice, Beto e Simão, possuem um par de chaves assimétricas, KR e KU, e as chaves públicas, KU_A, KU_B e KU_S, são de conhecimento de todos os elementos participantes do processo. Ou seja, a modelagem inicia-se no Passo (4) do protocolo proposto.

A ferramenta usada para modelagem em Redes de Petri é o *Analisador de Redes de Petri - ARP* [MAZ 90].

Para a análise do protocolo proposto, na seção A.1, apresenta-se a descrição formal do protocolo em Redes de Petri, usando a ferramenta ARP. Em seguida, na seção A.2, o resultado da análise é apresentado.

A.1 Descrição dos Elementos das Redes de Petri

Faz-se, nessa seção, a definição, a modelagem efetiva do protocolo proposto, usando Redes de Petri.

Para melhor visualização do protocolo proposto modelado em Redes de Petri ilustra-se, na Figura A.1, a representação gráfica da formalização descrita em ARP.

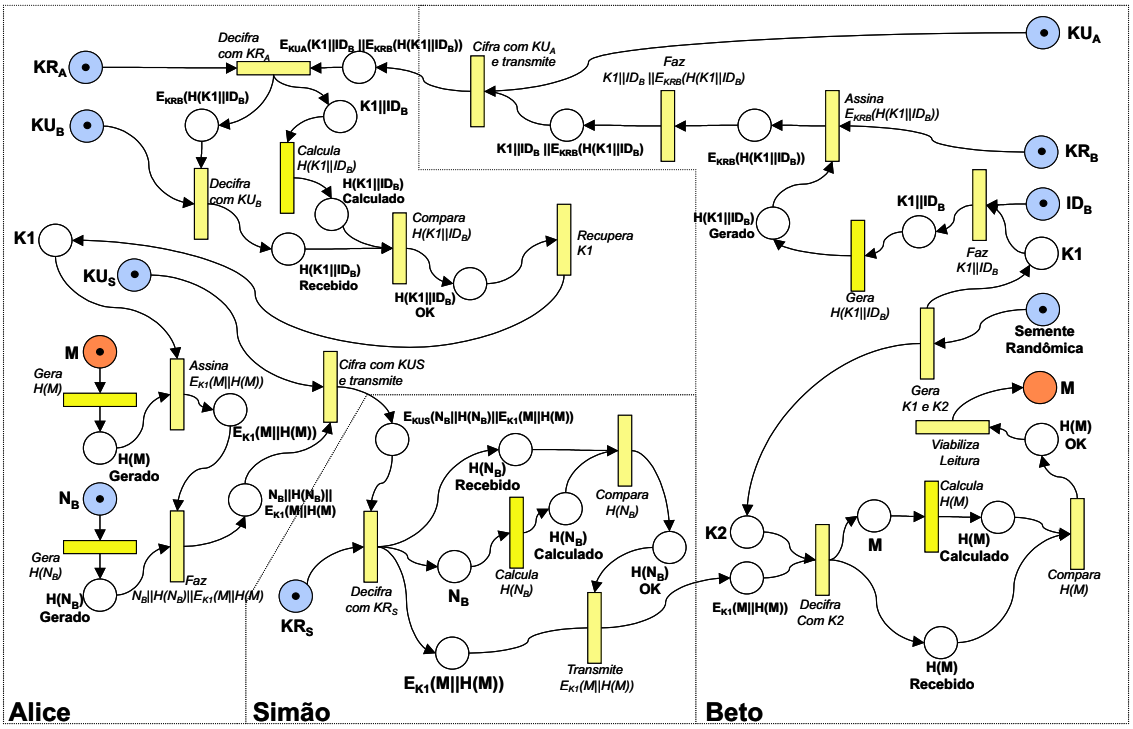

Figura A.1: Visualização Gráfica da Rede de Petri do Protocolo Proposto - Esta é a representação gráfica do protocolo proposto, modelado em Rede de Petri.

A descrição dos elementos de **Nós** (*nodes*), que define todos os **Lugares** e **Transições** na linguagem específica da ferramenta ARP, está representada na Figura A.2. Na seqüencia, apresenta-se a Figura A.3 com a estrutura da Rede de Petri, representada na linguagem ARP.

Faz-se, a seguir, a associação de cada um dos elementos da Rede de Petri, representados nas figuras A.2 e A.3, com os passos do protocolo proposto.

Passo (4) - Este passo consiste das seguintes ações:

1. Beto gera K_1 e K_2. Na linguagem ARP descrita tem-se o seguinte:

   $$Gera\_K1\_K2$$

   A pré-condição para que essa ação ocorra é que Beto possua uma semente randômica, ou seja:

   $$Semente\_Randomica = 1$$

   Como resultado tem-se o seguinte:

   $$Chave\_K1\_Gerado = 1$$

   $$Chave\_K2\_Gerado = 1$$

2. Beto encaminha a chave K_1 a Alice, por um canal seguro. Na linguagem ARP descrita tem-se o seguinte:

   $$Cifra\_KUA$$

   As pré-condições para que isso ocorra são as seguintes:

   - Beto deve possuir a chave pública de Alice, KU_A. Na representação em ARP, tem-se o seguinte:

   $$Chave\_KUA = 1$$

   - Beto deve possuir $H(K_1 \| ID\_B) \| E_{KR_B}(H(K_1 \| ID_B))$. Na representação em ARP, tem-se o seguinte:

   $$K1\_IDB + Ass\_KRB\_O = 1$$

   Para que está última pré-condição seja satisfeita, Beto faz o seguinte:

   a) Beto faz $K_1 \| ID_B$, representado por:

   $$Faz\_K1\_IDB$$

   b) Beto calcula $H(K_1 \| ID_B)$, representado por:

   $$Gera\_Hash\_K1\_IDB$$

   c) Beto cifra $H(K_1 \| ID_B)$ com sua chave privada, KR_B, representado por:

   $$Assina\_K1\_IDB\_KRB$$

   d) Beto faz $H(K_1 \| ID\_B) \| E_{KR_B}(H(K_1 \| ID_B))$, representado por:

   $$Faz\_K1\_IDB + Ass\_KRB$$

3. Para recuperar a chave K_1 recebida de Beto, as seguintes ações devem ser feitas por Alice:

   a) Alice recebe $E_{KU_A}(H(K_1\|ID\_B)\|E_{KR_B}(H(K_1\|ID_B)))$ de Beto. Na representação em ARP, tem-se o seguinte:

   $$K1\_IDB\_Cifrado\_KUA = 1$$

   b) Alice decifra $E_{KU_A}(H(K_1\|ID\_B)\|E_{KR_B}(H(K_1\|ID_B)))$ com sua chave privada, KR_A. Na representação em ARP, tem-se o seguinte:

   $$Decifra\_KRA$$

   c) Alice decifra o resumo assinado com KR_B recebido, $E_{KR_B}(H(K_1\|ID_B))$, recuperando $H(K_1\|ID_B)$. Na representação em ARP, tem-se o seguinte:

   $$Decifra\_KUB$$

   d) Alice calcula o resumo de $K_1\|ID_B$ recebido. Na representação em ARP, tem-se o seguinte:

   $$Calcula\_Hash\_K1\_IDB$$

   e) Alice compara o resumo recebido com o resumo calculado. Na representação em ARP, tem-se o seguinte:

   $$Compara\_Hash\_K1\_IDB$$

   f) Somente então, Alice recupera K_1. Na representação em ARP, tem-se o seguinte:

   $$Recupera\_K1$$

   Após essas ações, Alice possuirá a chave K_1, ou seja:

   $$Chave\_K1\_Recuperado = 1$$

Na representação feita neste apêndice, considera-se o uso das Redes de Misturadores. Sendo assim, os passos de número 5, 6, 7 e 8 não estão representados, indo direto ao Passo (9).

Passo (9) - Este passo consiste da seguinte ação:

- Alice envia a mensagem M cifrada com K_1, juntamente com o endereço de Beto, N_B, para Simão, por um canal seguro. Na representação ARP, para que isso possa

ocorrer, deve-se ter o seguinte:

$$M\_Cifrada\_KUS = 1$$

Para isso, Alice deve tomar as seguintes ações:

1. Alice gera o resumo da mensagem M, $H(M)$ e o resumo do endereço de Beto N_B, $H(N_B)$. Na representação em ARP, tem-se o seguinte:

   $$Gera\_Hash\_M$$

   $$Gera\_Hash\_NB$$

2. Alice cifra $M\|H(M)$ com K_1. Na representação em ARP, tem-se o seguinte:

   $$Assina\_M\_K1$$

3. Alice faz $H_B\|H(N_B)\|E_{K_1}(M\|H(M))$. Na representação em ARP, tem-se o seguinte:

   $$Faz\_NB\_HNB + M\_Ass\_K1$$

4. Alice cifra $H_B\|H(N_B)\|E_{K_1}(M\|H(M))$ com a chave pública de Simão, KU_S. Na representação em ARP, tem-se o seguinte:

   $$Cifra\_KUS\_T$$

   Nesse momento, o Passo (9) se completa, obtendo-se o seguinte:

   $$M\_Cifrada\_KUS = 1$$

Passo (10) - O processo se completa neste passo, onde a mensagem M é repassada por Simão a Beto.

Para isso, Simão deve fazer o seguinte:

1. Simão decifra a mensagem recebida de Alice com sua chave privada, KR_S. Na representação em ARP, tem-se o seguinte:

   $$Decifra\_KRS$$

2. Com isso, Simão decifra a informação $H_B\|H(N_B)$. Simão, então, calcula o resumo de N_B, $H(N_B)$. Na representação em ARP, tem-se o seguinte:

   $$Calcula\_Hash\_NB$$

3. Simão compara o resumo $H(N_B)$ recebido com o calculado. Na representação em ARP, tem-se o seguinte:

   $$Compara\_Hash\_NB$$

4. Simão, então, repassa a mensagem cifrada, $E_{K_1}(M \| H(M)$, para Beto. Na representação em ARP, tem-se o seguinte:

   $$Transmite\_M\_Ass\_K1$$

   Nesse momento, tem-se o seguinte:

   $$M\_Ass\_K1\_Beto = 1$$

Ao receber $E_{K_1}(M \| H(M)$ de Simão, Beto deve fazer o seguinte, para recuperar a mensagem M:

1. Beto decifra a mensagem recebida, $E_{K_1}(M \| H(M)$, com a chave privada K_2. Na representação ARP, tem-se o seguinte:

   $$Decifra\_K2$$

2. Em seguida, Beto calcula o resumo de M, $H(M)$, e compra com $H(M)$ recebido. Na representação ARP, tem-se o seguinte:

   $$Calcula\_Hash\_M$$

   $$Compara\_Hash\_M$$

3. Finalmente, a mensagem M é recebida e sua integridade é certificada por Beto. Na representação ARP, tem-se o seguinte:

   $$Leitura\_M$$

   Com isso, a mensagem M chega ao seu destino. Na representação ARP, tem-se o seguinte:

   $$Mensagem\_M\_Destino = 1$$

A.2 Resultado Obtido

Verificou-se e atestou-se a conformidade do protocolo proposto fazendo-se uso da formalização do mesmo em Rede de Petri. Apresenta-se, ainda, algumas telas

ilustrativas, com os resultados extraídos da ferramenta de modelagem ARP.

Na primeira tela, ilustrada na Figura A.4, apresenta-se o resultado da compilação do protocolo modelado. Na segunda tela, ilustrada na Figura A.5, apresenta-se o estado inicial da rede, com os nós *lugares* que possuem uma marca inicial 1.

Diante das condições iniciais, as três únicas transições possíveis de serem feitas são: *Gera-Hash-M*, *Gera-Hash-NB* e *Gera-K1-K2*. Nenhuma das outras ações poderão ser tomadas, sem que antes se faça pelo menos uma das transições citadas acima. A terceira tela, ilustrada na Figura A.6, apresenta as transições possíveis nesse ponto.

As 24 transições vão se sucedendo adequadamente e, após a execução da última transição *Leitura-M*, o nó *Mensagem-M-Destino* é marcada com 1, indicando que a mensagem chegou a seu destino, conforme a proposta do protocolo. Confirma-se, então, o sucesso na seqüência das transições necessárias, ou seja, todos os passos do protocolo se efetivaram sem a existência de entraves. A tela da Figura A.7 ilustra a finalização adequada do processo.

A.3 Conclusão

Fez-se, neste apêndice, a modelagem formal do protocolo proposto em Redes de Petri. Com isso, pôde-se avaliar a seqüência de passos seguidos no protocolo, incluindo os paralelismos existentes, validando a corretude da interdependência dos passos. Como resultado, constatou-se a inexistência de entraves ou bloqueios que, porventura, poderiam vir a ocorrer.

Além disso, a representação do protocolo em um modelo formal, sendo este as Redes de Petri ou qualquer outro, facilita o entendimento de especialistas da área que, conhecendo o modelo utilizado, poderão mais facilmente entender a mecânica do protocolo.

```
Nodes

        { Alice }
        Mensagem_M_Origem       :       Place (1);
        Endereco_Beto_NB        :       Place (1);
        Chave_KRA               :       Place (1);
        Chave_KUB               :       Place (1);
        Chave_KUS               :       Place (1);
        Hash_M_Gerado           :       Place;
        Hash_NB_Gerado          :       Place;
        NB_HNB+M_ass_K1         :       Place;
        M_Ass_K1_Alice          :       Place;
        Chave_K1_Recuperado     :       Place;
        K1_IDB_Cifrado_KUA      :       Place;
        K1_IDB_Ass_KRB_D        :       Place;
        K1_IDB_Destino          :       Place;
        Hash_K1_IDB_Calc        :       Place;
        Hash_K1_IDB_Rec         :       Place;
        Hash_K1_IDB_OK          :       Place;
        Gera_Hash_M             :       Transition;
        Gera_Hash_NB            :       Transition;
        Assina_M_K1             :       Transition;
        Faz_NB_HNB+M_ass_K1     :       Transition;
        Cifra_KUS_T             :       Transition;
        Decifra_KRA             :       Transition;
        Decifra_KUB             :       Transition;
        Calcula_Hash_K1_IDB     :       Transition;
        Compara_Hash_K1_IDB     :       Transition;
        Recupera_K1             :       Transition;

        { Simao }
        Chave_KRS               :       Place (1);
        M_Cifrada_KUS           :       Place;
        Hash_NB_Recebido        :       Place;
        Hash_NB_Calculado       :       Place;
        NB_Recebido             :       Place;
        M_Ass_K1_Simao          :       Place;
        Hash_NB_OK              :       Place;
        Decifra_KRS             :       Transition;
        Calcula_Hash_NB         :       Transition;
        Compara_Hash_NB         :       Transition;
        Transmite_M_Ass_K1      :       Transition;

        { Beto }
        Chave_KUA               :       Place (1);
        Chave_KRB               :       Place (1);
        Identidade_Beto_IDB     :       Place (1);
        Semente_Randomica       :       Place (1);
        Chave_K1_Gerado         :       Place;
        Chave_K2_Gerado         :       Place;
        M_Ass_K1_Beto           :       Place;
        Mensagem_M_Recebido     :       Place;
        Mensagem_M_Destino      :       Place;
        Hash_M_Recebido         :       Place;
        Hash_M_Calculado        :       Place;
        Hash_M_OK               :       Place;
        K1_IDB_Origem           :       Place;
        Hash_K1_IDB_Gerado      :       Place;
        K1_IDB_Ass_KRB_O        :       Place;
        K1_IDB+Ass_KRB          :       Place;
        Decifra_K2              :       Transition;
        Calcula_Hash_M          :       Transition;
        Compara_Hash_M          :       Transition;
        Leitura_M               :       Transition;
        Gera_K1_K2              :       Transition;
        Faz_K1_IDB              :       Transition;
        Gera_Hash_K1_IDB        :       Transition;
        Assina_K1_IDB_KRB       :       Transition;
        Faz_K1_IDB+Ass_KRB      :       Transition;
        Cifra_KUA               :       Transition;
```

Figura A.2: Descrição dos Lugares e Transições em Linguagem ARP - Essa figura apresenta a descrição dos elementos, Lugares e Transições, definidos na formalização do protocolo proposto em Redes de Petri, na formatação específica da ferramenta ARP.

```
Structure { Protocolo }

        { Alice }
        Gera_Hash_M             :       (Mensagem_M_Origem),
                                        (Hash_M_Gerado);
        Gera_Hash_NB            :       (Endereco_Beto_NB),
                                        (Hash_NB_Gerado);
        Assina_M_K1             :       (Hash_M_Gerado,
                                         Chave_K1_Recuperado),
                                        (M_Ass_K1_Alice);
        Faz_NB_HNB+M_ass_K1     :       (Hash_NB_Gerado,
                                         M_Ass_K1_Alice),
                                        (NB_HNB+M_ass_K1);
        Cifra_KUS_T             :       (NB_HNB+M_ass_K1,Chave_KUS),
                                        (M_Cifrada_KUS);
        Decifra_KRA             :       (K1_IDB_Cifrado_KUA,Chave_KRA),
                                        (K1_IDB_Ass_KRB_D,K1_IDB_Destino);
        Decifra_KUB             :       (K1_IDB_Ass_KRB_D,Chave_KUB),
                                        (Hash_K1_IDB_Rec);
        Calcula_Hash_K1_IDB     :       (K1_IDB_Destino),
                                        (Hash_K1_IDB_Calc);
        Compara_Hash_K1_IDB     :       (Hash_K1_IDB_Rec,Hash_K1_IDB_Calc),
                                        (Hash_K1_IDB_OK);
        Recupera_K1             :       (Hash_K1_IDB_OK),
                                        (Chave_K1_Recuperado);

        { Simao }
        Decifra_KRS             :       (M_Cifrada_KUS,Chave_KRS),
                                        (Hash_NB_Recebido,NB_Recebido,
                                         M_Ass_K1_Simao);
        Calcula_Hash_NB         :       (NB_Recebido),
                                        (Hash_NB_Calculado);
        Compara_Hash_NB         :       (Hash_NB_Recebido,Hash_NB_Calculado),
                                        (Hash_NB_OK);
        Transmite_M_Ass_K1      :       (M_Ass_K1_Simao,Hash_NB_OK),
                                        (M_Ass_K1_Beto);

        { Beto }
        Decifra_K2              :       (M_Ass_K1_Beto,Chave_K2_Gerado),
                                        (Mensagem_M_Recebido,
                                         Hash_M_Recebido);
        Calcula_Hash_M          :       (Mensagem_M_Recebido),
                                        (Hash_M_Calculado);
        Compara_Hash_M          :       (Hash_M_Recebido,Hash_M_Calculado),
                                        (Hash_M_OK);
        Leitura_M               :       (Hash_M_OK),
                                        (Mensagem_M_Destino);
        Gera_K1_K2              :       (Semente_Randomica),
                                        (Chave_K1_Gerado,Chave_K2_Gerado);
        Faz_K1_IDB              :       (Chave_K1_Gerado,
                                         Identidade_Beto_IDB),
                                        (K1_IDB_Origem);
        Gera_Hash_K1_IDB        :       (K1_IDB_Origem),
                                        (Hash_K1_IDB_Gerado);
        Assina_K1_IDB_KRB       :       (Hash_K1_IDB_Gerado,Chave_KRB),
                                        (K1_IDB_Ass_KRB_O);
        Faz_K1_IDB+Ass_KRB      :       (K1_IDB_Ass_KRB_O),
                                        (K1_IDB+Ass_KRB);
        Cifra_KUA               :       (K1_IDB+Ass_KRB,Chave_KUA),
                                        (K1_IDB_Cifrado_KUA);
```

Figura A.3: Estrutura da Rede de Petri do Protocolo Proposto em ARP - Apresenta-se a estrutura da Rede de Petri que formaliza o protocolo proposto, na linguagem ARP.

Figura A.4: Ilustração do Resultado da Compilação - Essa é a tela da ferramenta ARP, representando o resultado positivo da compilação, com 39 nós lugares e 24 nós transições.

Figura A.5: Tela Apresentando o Estado Inicial da Rede - Essa tela apresenta o estado inicial da Rede, com os nós lugares que possuem uma marca inicial 1.

Figura A.6: Transições Possíveis a Partir do Estado Inicial - Essa tela apresenta as transições possíveis a partir do estado inicial da Rede.

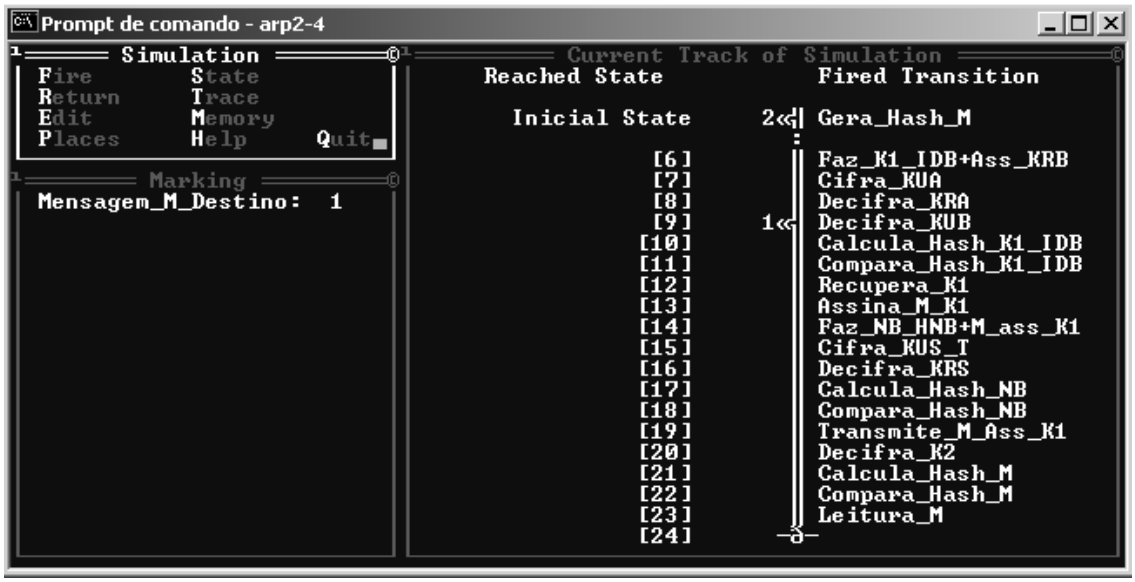

Figura A.7: Tela Apresentando a Chegada da Mensagem ao seu Destino - Essa tela representa a chegada da mensagem a seu destino, em conformidade com a proposta do protocolo, simbolizada pela marca $Mensagem\_M\_Destino : 1$.